

SECURITY PROOF OF QUANTUM KEY DISTRIBUTION WITH DETECTION EFFICIENCY MISMATCH

CHI-HANG FRED FUNG¹, KIYOSHI TAMAKI²
BING QI³, HOI-KWONG LO³, and XIONGFENG MA⁴

¹*Department of Physics and Center of Computational and Theoretical Physics,
University of Hong Kong, Pokfulam Road, Hong Kong, China*

²*NTT Basic Research Laboratories, NTT Corporation,
3-1, Morinosato Wakamiya Atsugi-Shi, Kanagawa, 243-0198, Japan;
CREST, JST Agency, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

³*Center for Quantum Information and Quantum Control,
Department of Physics and Department of Electrical & Computer Engineering,
University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

⁴*Institute for Quantum Computing, University of Waterloo,
200 University Ave. W., Waterloo, Ontario, N2L 3G1, Canada*

Received (received date)

Revised (revised date)

In theory, quantum key distribution (QKD) offers unconditional security based on the laws of physics. However, as demonstrated in recent quantum hacking theory and experimental papers, detection efficiency loophole can be fatal to the security of practical QKD systems. Here, we describe the physical origin of detection efficiency mismatch in various domains including spatial, spectral, and time domains and in various experimental set-ups. More importantly, we prove the unconditional security of QKD even with detection efficiency mismatch. We explicitly show how the key generation rate is characterized by the maximal detection efficiency ratio between the two detectors. Furthermore, we prove that by randomly switching the bit assignments of the detectors, the effect of detection efficiency mismatch can be completely eliminated.

Keywords: Quantum cryptography, quantum key distribution, security proof, detection efficiency mismatch

1 Introduction

Quantum key distribution (QKD) [1–3] provides a way for two legitimate users, Alice and Bob, to share a secret key that is secure against an eavesdropper, Eve, who is only restricted by quantum mechanics. After the successful sharing of the secret key, Alice and Bob can

then use it in cryptographic applications such as secure communications and authentication. Many previous unconditional security proofs for QKD [4–15] consider the case with perfect devices, such as perfect single-photon sources. However, realistic devices are never perfect. For example, weak coherent sources are widely used in practice to simulate single-photon emissions. Thus, security proofs have to be extended to cover these practical imperfections in order to guarantee the security of a practical system. Recently, the use of weak coherent sources and threshold detectors have been considered by various security proofs [16–22]. In this paper, we consider another realistic imperfection found in detectors, which is the dependency of detection efficiency on some auxiliary dimension such as the arrival time of signal; furthermore, the efficiencies of the two detectors can be different. We prove the unconditional security for this case. In this paper, we consider a QKD scheme where Bob uses two separate detectors for detecting bits “0” and “1”.

The general physical problem we are facing in practical QKD system with two detectors is the detection efficiency loophole [23, 24]. This loophole underlies not only fundamental physics like Bell inequalities, but also applied technology like QKD. Also, in practice, it is hard to build two detectors that have exactly the same characteristics (e.g. frequency, time and spatial responses). Moreover, the problem of detection efficiency mismatch is important not only for gated detectors, but also for detectors with dead-times. Indeed, standard InGaAs detectors (and even SSPDs) have dead-times. That is to say that after a detection event, a detector becomes inactive for some prescribed time duration. If Bob registers a signal during a time period when one detector is dead while the other one is still active, Eve will be able to infer which detector clicks. Our paper is an illustration of how one can proceed to handle this general problem of detection efficiency mismatch in the security of QKD.

In fact, attacks drawing on detection efficiency mismatch have been proposed before: the faked states attack [25, 26] and the time-shift attack [27]. The faked-states attack [25, 26] is an intercept-and-resend attack, which is challenging to implement because of synchronization and interferometric stability issues. For this reason, the faked-states attack has never been implemented experimentally. In contrast, the time-shift attack [27] does not involve any measurement and is, therefore, easier to implement in this regard. Indeed, we have successfully demonstrated the time-shift attack experimentally on a commercial QKD system [28], which indicates that detection efficiency mismatch is a serious realistic issue that can have a fatal effect on practical security^a.

The success of the faked-states attack and the time-shift attack relies on the existence of detection efficiency mismatch and the assumption that Alice and Bob distill keys using a standard security proof that ignores this efficiency mismatch. As we have noted before [28, 30], once Alice and Bob are aware of an attack based on some imperfection, it may not be too difficult for them to devise counter measures against it. On the other hand, counter-measures against eavesdropping can often lead to new loopholes and/or be defeated by new eavesdropping attacks. For instance, the four-state setting [31, 32] by Bob (intended to counter

^a Note that to implement the time-shift attack successfully, one may need to implement time compression of signals. The signals being compressed here are strong classical pulses from Bob to Alice in a plug-and-play system. Fortunately, compression of strong classical pulses is a mature standard technique that has been used in industries for decades (see, e.g., [29]). For simplicity, the experiment in Ref. [28] did not implement this mature standard technique but simulated this compression process by replacing the original laser source with one that produces narrower pulses.

attacks based on detection efficiency mismatch) can be defeated by a combination of the large-pulse attack [33] and the time-shift attack [30, 34]. Instead of implementing physical countermeasures, another way to guard against attacks based on detection efficiency mismatch is for Alice and Bob to take this imperfection into account when distilling keys. Because of this imperfection, an extra amount of privacy amplification will be needed. In this paper, we provide an unconditional security proof that takes detection efficiency mismatch into account, and by using this proof, Alice and Bob will be able to determine the right amount of privacy amplification needed to remove Eve's information on the final key even in the presence of detection efficiency mismatch. We note that our proof is valid even if Eve performs the most general attack that correlates different signal transmissions.

In this paper, we consider the BB84 protocol [1], but the idea of our security proof can be used for other protocols. For simplicity, for much of this paper, we consider that the input to Bob are single-photon signals. The case of multi-photon input signals will be discussed in Sec. 7.1. For each transmission by Alice, Eve resends two systems to Bob: one system carrying the bit information and the other system representing the auxiliary system that the efficiencies of the detectors respond to. We assume in this paper that the information-carrying system is a qubit. On the other hand, the auxiliary system can have arbitrary dimension and is completely controlled by Eve in order to produce different effects on Bob due to imperfect detection efficiencies. More specifically, Eve can send Bob an arbitrary state in this auxiliary system to induce different probabilities of detection for the two detectors. Overall, Bob's system is represented by an enlarged quantum space and the bit information only lives in a qubit subspace of it. Thus, our security proof is one that applies to a protocol with an enlarged quantum space (which has recently been formalized in Ref. [35]). Also, we note that this auxiliary system essentially acts as a shield [36] that protects Alice and Bob's key from Eve. Thus, our proof serves as an example of shield analysis.

Bob's measurement operates on both the qubit system (which carries the information) and the auxiliary system (which affects the detection efficiencies) and we need a detector model that incorporates both systems. In this paper, we do not attempt to treat the most general measurements but to assume a slightly more restrictive detector model that does not couple the two systems. In other words, our model applies whenever the information-carrying dimension does not couple with the efficiency-affecting dimension in the detection process. This detector model by no means covers all possible detection scenarios^b but is general enough to include many interesting ones (such as those described in Sec. 2) that arise in practice. It is important to note that even though the detector model does not couple the two systems, they can be arbitrarily coupled (entangled) in the input state sent by Eve.

To get a glimpse at our detector model, let's first consider the case where there is no Eve and no efficiency mismatch. In this case, the entanglement view of Alice's and Bob's systems is simply the perfect EPR pair $|00\rangle_{AB} + |11\rangle_{AB}$. Now, supposing that there is efficiency mismatch and each detector i has a constant efficiency η_i , the state can then be represented as $\sqrt{\eta_0}|00\rangle_{AB} + \sqrt{\eta_1}|11\rangle_{AB}$, which can be regarded as a non-uniform EPR pair. This simple case is a special case of what we consider in our security proof. In fact, we consider a detector model that goes beyond the scalar efficiency model. Our model can incorporate, for example, states of the form $|00\rangle_{AB} \otimes (F_0|\gamma\rangle_T) + |11\rangle_{AB} \otimes (F_1|\gamma\rangle_T)$, where F_i is the filtering operation

^bFor instance, our detector model does not cover the case when Bob's Hilbert space is a qutrit.

of detector i acting on system T modeling the detector's efficiency response and $|\gamma\rangle$ is an arbitrary state chosen by Eve to induce different effects on the two detectors. The difficulty in proving the security is related to the non-uniformity in bits "0" and "1" of the overall state and the fact the initial state in system T is arbitrary. Nevertheless, we propose a technique that proves the security even though Eve can choose any state in system T .

Our proof considers that Alice uses a single-photon source. However, our result immediately applies to the case when Alice uses a phase-randomized weak coherent source, by using the results of Ref. [17, 18]. Our proof is founded on Koashi's general security proof based on the uncertainty principle [18]. The essential strategy is to estimate how certain Bob can predict Alice's measurement outcomes in the basis conjugate to the key-generating basis. To do this, we consider a virtual protocol in which Bob performs a virtual measurement on his enlarged quantum space where the information-carrying qubit is embedded. His measurement result then gives a good prediction of Alice's.

Intuition tells us that the larger the mismatch between the two detectors is, the lower the key generation rate becomes. We confirm this belief in our paper and explicitly quantify the exact effect of the mismatch on the key generation rate. We show that the maximum efficiency ratio between the two detectors is directly related to the key generation rate [see Eqs. (27), (28), and (31)].

There has been much interest in security proofs of QKD based on fundamental principles such as no-signaling faster than the speed of light and Bell's inequality violations [37, 38]. In particular, the idea of device-independent security proofs has been proposed. So far a complete proof of security along this line is still missing and such a proof idea only applies to specialized attacks such as collective attacks. We remark that this paper, following our earlier time-shift attack papers [27, 28], serves to highlight a fundamental weakness of device-independent security proof. Even if such a proof can be constructed in future for the most general attack, it will *not* apply to most current practical QKD set-ups. This is because of the existence of detection efficiency loophole and Eve's potential ability to manipulate signals in the auxiliary domain to bias the relative detection efficiency between two detectors. (Notice, however, that, as we will show in Sec. 6, a four-phase setting idea can equalize the detection efficiency of two detectors.)

This paper is organized as follows. In Sec. 2, we give an overview of the physical origin of detection efficiency mismatch and how Eve might exploit this mismatch. We then introduce our detector model in Sec. 3. In Sec. 4, we consider the security proof for the noiseless case, in which Eve does not introduce any bit or phase errors but only intervenes with the auxiliary dimension. The study of the noiseless case is instructive as it illustrates clearly our proof technique that is shared across both the noiseless and noisy cases. In Sec. 5, we provide the unconditional security proof for the noisy case, in which Eve introduces bit and phase errors, in addition to intervening with the auxiliary dimension. In Sec. 6, we show how randomly switching the bit assignments of the two detectors for each quantum signal (similar to the scheme proposed by Refs. [31, 32]) can completely eliminate the effect of detection efficiency mismatch. In Sec. 7, we discuss how to handle multi-photon signals in our proof, with the help of the results of other papers. Finally, we conclude in Sec. 8.

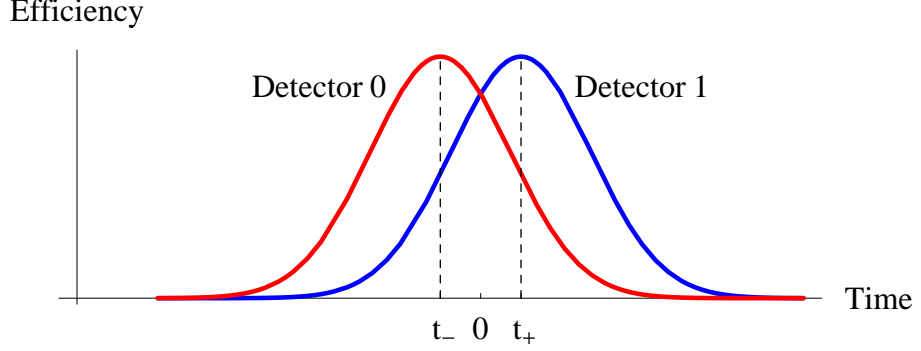


Fig. 1. Mismatch in efficiency between two detectors. Due to the asymmetry between the two detection channels the time responses of the two detectors may not be identical. Under normal operation, signals are expected to arrive at time 0. On the other hand, Eve can launch a “time-shift attack” in which she shifts the arrival times of the signals to say times t_- or t_+ in order to subject the signals to different probabilities of being detected as bit “0” or bit “1”. Thus, because of this difference in the detection probabilities of bit “0” and bit “1”, Eve can learn some information about the key.

2 Practical detection efficiency mismatch and attacks

In this section, we consider detection efficiency mismatch in realistic QKD setups and possible attack strategies that are based on detection efficiency mismatch. Without a security proof that takes into account of detection efficiency mismatch, these attacks may compromise the security of QKD systems. The security proof provided later in this paper takes detection efficiency mismatch into account and allows Alice and Bob to defeat these attacks.

2.1 Time-domain detection efficiency mismatch

In a typical fiber-based QKD system operating at 1550nm wavelength, in order to minimize the effect of dark counts, the two InGaAs detectors are usually gated to be active in a narrow time window in which signals are expected to arrive. However, due to the different responses of the two detectors and also the asymmetry between the two detection channels, the detectors may have different efficiencies over time. Fig. 1 illustrates a mismatch in efficiency between two detectors. Typically, the open windows of the two detectors are larger than the width of the laser pulses. Thus, under normal operation, the signals arrive near the centre of the two open windows so that the efficiencies for detecting bit “0” and bit “1” are similar. However, it is possible for Eve to time shift the input signals to Bob causing a mismatch in the efficiencies. In Ref. [27], we proposed a “time-shift attack” that basically draws on this efficiency mismatch due to time shifting. Essentially, Eve time shifts the signals entering Bob to say time t_- . Whenever Bob announces that he has a detection, Eve knows that it is likely that detector 0 has clicked because it has a higher efficiency at time t_- . Thus, Eve obtains some information about the bit value. In the extreme case that at a particular time shift, the efficiency of one detector is positive and efficiency of the other detector is zero, Eve knows the bit value exactly because only one detector can ever produce a click. Standard security proofs that ignore efficiency mismatch may allow Eve to steal information in this way. On the other hand, the security proof provided in this paper takes this mismatch into account and applies

enough privacy amplification depending on the mismatch to remove Eve's information. We remark that a successful experimental demonstration of this attack has been performed by us [28].

Note that when multiple pulses arrive in the same detection window, the efficiency of the detection system may depend on the relative phases of these multiple pulses. This may happen when there exist multiple reflection sites in the detection channel. We will establish a detector model in Sec. 3 that is general enough to incorporate this correlation.

2.2 *Space-domain detection efficiency mismatch*

The space-domain efficiency mismatch is related to free-space QKD systems [39–46] where a change in the spatial mode of the input light may affect the efficiencies of the two detection channel differently. In order to illustrate this concept, we show in Fig. 2 a simple detection setup. Here, the two output lights of the beamsplitter pass through the optical coupling systems before being detected. In practice, there exists asymmetry between the two free-space to fiber coupling systems. For example, the distances between the coupling systems and the beamsplitter may not be identical and also the lenses of the coupling systems may not be perfectly aligned with respect to the beamsplitter. If Eve changes the spatial mode of the input laser beam (e.g., angle, lateral displacement), the losses in the two coupling systems can potentially be different, leading to detection efficiency mismatch which Eve can take advantage of. Let's consider an extreme example. Suppose that the two single-photon detectors (SPD's) are identical, but the distance from the collecting lens of channel 1 to the beamsplitter is twice the distance from the collecting lens of channel 2 to the beamsplitter (see Fig. 2). In this case, if Eve changes the angle of the input laser beam, the resulting lateral displacement of the laser beam at the surface of the lens of channel 1 is twice that at the surface of the lens of channel 2. Thus, this induces higher efficiency for channel 2 than for channel 1. In free-space QKD setups, four detectors are often used with passive basis selection. In this case, it is conceivable that Eve manipulates the spatial mode of each signal and thereby produces a bias towards one basis use.

In practice, the process of free-space optical alignment is quite complicated, with many factors contributing to the coupling efficiency. Also, errors in the manufacturing process of optical elements can lead to variations in the coupling efficiency. Spatial change to the input laser beam can further enhance the variations. Thus, it is expected that a spatial attack can be used to effectively create efficiency mismatch. Also, note that coupling efficiency mismatch does not vary with time, which liberates Eve from dealing with time-dependent issues.

2.3 *Frequency-domain detection efficiency mismatch*

In a similar way, detectors may respond to different wavelengths with different efficiencies. Thus, in principle, Eve may shift the frequency of the incoming signals at Bob to launch her attack. An acousto-optic modulator can be used to shift the frequency of the input signal up to a few GHz. On the other hand, by employing nonlinear optical materials, the wavelength of light can be shifted by a few hundreds nm [47].

Wavelength filters can be used to ensure that only photons within certain spectral band are permitted to reach the SPD's. However, one must be careful about the placements of the filters. If a separate filter is placed before each SPD, Eve may still be able to exploit some efficiency mismatch, since the spectral responses of the two wavelength filters may not

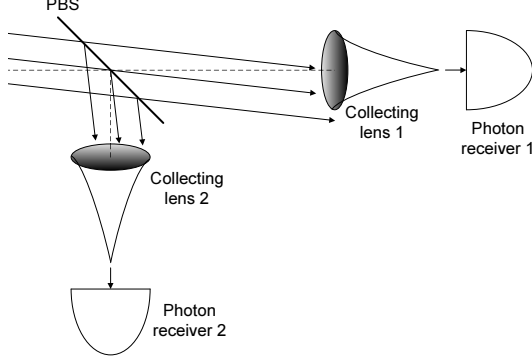


Fig. 2. Eve changes the incident angle of the input laser beam. Since the distance between collecting lens 1 and the beamsplitter is not the same as the distance between collecting lens 2 and the beamsplitter, the laser beam arrives at different lateral displacements on the surfaces of the collecting lenses, causing different losses and in turn a mismatch in the detection efficiencies. Thus, because of this difference in the detection probabilities of bit “0” and bit “1”, Eve may learn some information about the key if Alice and Bob are not aware of this mismatch.

fully overlap and thus shifting in frequency may still lead to different efficiencies. Thus, one simple counter measure is to place one wavelength filter at the entrance of Bob’s system. Conventional SPD’s based on Si-APD or InGaAs-APD have a spectral response range of a few hundreds nanometer, while the bandwidth of a narrow-band filter may be 1 nm. Thus, the responses of the SPD’s may be regarded as identical. On the other hand, other types of SPD’s, such as the up-conversion SPD’s, may have a bandwidth less than 1 nm due to the requirement of phase matching in the up-conversion process. In this case, a wavelength filter with a bandwidth of 1 nm may not be able to eliminate the efficiency mismatch and the SPD’s may still respond differently to photons with different wavelengths (especially when the wavelengths of the input photons get close to the edge of the spectral response window); thus, a spectral attack may still be possible.

3 A general detector model

In this section, we describe a model for detectors in a QKD system that is general enough to cover a wide variety of efficiency dependencies. Our security proof with efficiency mismatch taken into account will be built on this detector model. Fig. 3 shows a QKD system with two detectors having efficiencies dependent on some auxiliary dimension (which, in this case, is time). We are interested in constructing a POVM (positive-operator-valued measurement) for Bob’s detector package for detecting bit “0” and bit “1”, taking into account the imperfect efficiencies. Bob’s detector package accepts two systems as input: system B for the qubit representing the information-carrying qubit state of the QKD protocol, and system T representing the auxiliary domain (e.g. time, space, and frequency) related to the detection efficiency.

Before we begin the construction of the POVM of Bob’s detector package, we state a few assumptions. We assume in the proof that Eve always sends single-photon signals to Bob (see also Sec. 7.1 for handling multi-photon input signals). Furthermore, she sends Bob a qubit state in system B . Dark counts in the detectors may be modeled by Eve sending

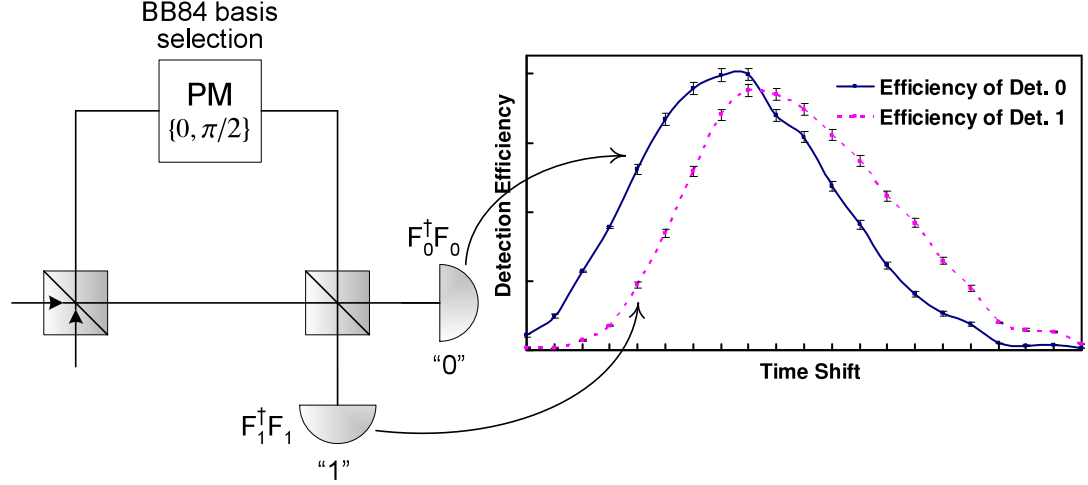


Fig. 3. There are two detectors in the QKD system, one for detecting bit “0” and the other for detecting bit “1”. The two detectors have different efficiencies and their efficiency responses are characterized by matrices $F_0^\dagger F_0$ and $F_1^\dagger F_1$. In this example, the efficiencies depend on the arrival time of the incoming signals, and the diagonal elements of $F_i^\dagger F_i$ expressed in the basis that represents the arrival times are plotted in the figure on the right. The data of this figure comes from an actual experiment that we performed to demonstrate the time-shift attack [28].

random qubits. In addition, we assume that in the detector model there is no coupling between the information-carrying qubit system and the auxiliary system. This means that in the detection process, information decoding operations (such as beam splitting) on the qubit system is not affected by the auxiliary system. This model is not the most general one but is consistent with the three detection scenarios we described in Sec. 2. This can be seen by noting that information bits “0” and “1” (encoded in polarization or phase) are discerned by a beam splitter separating the incoming signal into two paths, and the beam splitter acts independently of the arrival time, frequency, or spatial mode of the signal. Thus, we can assume that the POVM elements take a tensor product form in the qubit system and the auxiliary system.

We now characterize the POVM of the whole detector package consisting of two detectors. Let’s first focus on the Z -basis measurement by Bob. In this case, the POVM elements for measuring bit “0” and bit “1” can be represented by

$$M_0 = |0_z\rangle_B \langle 0_z| \otimes (F_0^\dagger F_0)_T \quad (1)$$

$$M_1 = |1_z\rangle_B \langle 1_z| \otimes (F_1^\dagger F_1)_T \quad (2)$$

where $F_i^\dagger F_i$ represents the efficiency matrix of detector i that we will discuss in the following. Thus, the POVM of Bob’s measurement is $\{M_0, M_1, \mathbb{I} - M_0 - M_1\}$, where the last element represents the case of not getting a click by Bob. In the special case that the two detectors have constant efficiencies, $F_i^\dagger F_i = \eta_i$ becomes a scalar and Bob’s POVM elements for conclusive events become $M_i = \eta_i |i_z\rangle_B \langle i_z|$, $i = 0, 1$. For the later use, it is convenient to express Bob’s measurement as a filtering operation followed by a simple measurement. The filtering is

$$F_z = |0_z\rangle_B \langle 0_z| \otimes (F_0)_T + |1_z\rangle_B \langle 1_z| \otimes (F_1)_T \quad (3)$$

and it is followed by the measurement $\{|0_z\rangle_B \langle 0_z| \otimes \mathbb{I}_T, |1_z\rangle_B \langle 1_z| \otimes \mathbb{I}_T\}$. In a similar way, Bob's X -basis measurement can be defined as the filtering operation

$$F_x = |+\rangle_B \langle +| \otimes (F_0)_T + |-\rangle_B \langle -| \otimes (F_1)_T, \quad (4)$$

followed by the measurement $\{|+\rangle_B \langle +| \otimes \mathbb{I}_T, |-\rangle_B \langle -| \otimes \mathbb{I}_T\}$. In Eqs. (1)-(4), we have ignored the possibility of double click events, in view of their low probabilities. However, as noted in ILM [16] and GLLP [17], one should assign random probabilities to double click events.

The POVM corresponding to detector i consists of two outcomes $\{F_i^\dagger F_i, I - F_i^\dagger F_i\}$, where the first (second) element corresponds to having (not having) a detection. Thus, when the input to detector i is ρ in the auxiliary domain, the probability of detection is $\text{Tr}(\rho F_i^\dagger F_i)$. In general, the efficiency response $F_i^\dagger F_i$ is a full matrix:

$$F_i^\dagger F_i = \begin{bmatrix} \eta_i(t_1, t_1) & \cdots & \eta_i(t_1, t_d) \\ \vdots & & \vdots \\ \eta_i(t_d, t_1) & \cdots & \eta_i(t_d, t_d) \end{bmatrix}. \quad (5)$$

This is because there may be a natural or convenient basis to represent it (e.g. F_i may be expressed in the basis in which one tests the detectors). Here, we assume that the auxiliary domain has a finite dimension d and it is known to Alice and Bob. Also, note that the two detectors may not be diagonalizable in the same basis.

One example of the auxiliary domain is the arrival time of the signal (see Fig. 3). The efficiency of gated single-photon detectors can be sensitive to the arrival time of the signals and the efficiency response $F_i^\dagger F_i$ is conveniently represented in the basis of arrival times. Thus, one may regard the diagonal term $\eta_i(t_j, t_j)$ as the efficiency of detector i at time t_j , and the dimension d is the number of allowable time shifts.

In many cases, one may completely characterize the detectors' responses F_i (with both diagonal and off-diagonal terms). For example, when the auxiliary domain is polarization, the dimensions of F_i is 2×2 , and its elements can be found by sending signals to the detector with vertical polarization, horizontal polarization, and the in-phase and out-of-phase superpositions of vertical and horizontal polarizations. On the other hand, when the auxiliary domain is time, there would be infinitely many uncountable time shifts and the dimensions of F_i would be infinite. Thus, it may appear that perfect characterization is difficult. However, with a small adjustment, the case of time-dependent efficiency can still be treated with finite dimensions, as we discuss next.

3.1 Time-dependent efficiency

3.1.1 Characterization with a finite number of samples

Let us consider that the detectors have an efficiency dependent on the arrival time of the signals. This is the case for detectors operating in gated Geiger mode (e.g., see our experimental time-shift attack paper [28] for how practical efficiency mismatch is exploited by Eve). When time is the auxiliary dimension, the efficiency response matrix $F_i^\dagger F_i$ becomes continuous and contains uncountable elements. This may be problematic to our analysis. However, with an additional minor assumption, this problem can be resolved and we can characterize $F_i^\dagger F_i$ with a finite number of elements.

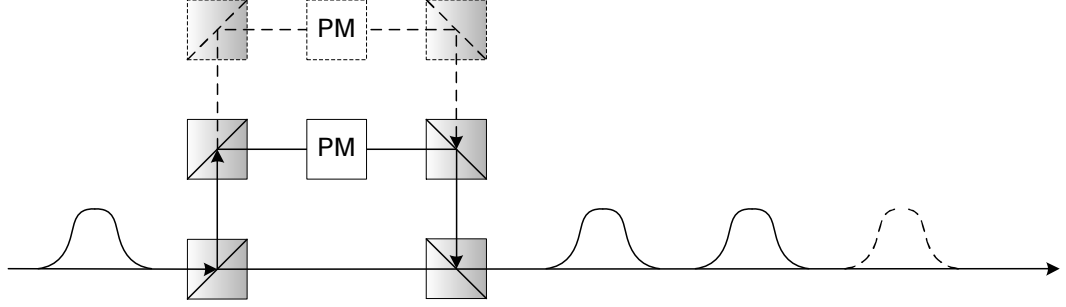


Fig. 4. An input signal can be split into more than one pulse by using beamsplitters. The phase modulators control the the relative phases between these multiple pulses. One may repeat this setup many times to get a superposition of many pulses.

The key assumption is that a narrow-band Gaussian-shaped frequency filter is installed at the entrance of Bob, with the center frequency matching that of the quantum signal. Thus, the incoming signals are filtered before reaching the detectors. The main idea is that the signal after the narrow-band filter must also be narrow-band. Thus, according to the Nyquist-Shannon sampling theorem [48], a narrow-band signal can be fully represented by its discrete samples. This means that the input to the detector can always be represented by a series of pulses located at fixed time instants, and thus this allows us to characterize the efficiency response of the detector only at those fixed time instants. Furthermore, when we consider the gating window to have a fixed length, we can characterize the detector with a finite number of pulses sent within the gating window. Therefore, with an addition of a frequency filter, the characterization of the time-dependent efficiency of the detectors becomes discrete and finite-dimensional, and thus is readily applicable to our security proof. The details are analyzed in Appendix A. Note that the use of a Gaussian-shaped frequency filter facilitates the use of Gaussian pulses to test the detectors, and Gaussian pulses are easy to generate in practice. By the same token, adding a time filter makes the characterization of frequency-dependent efficiency discrete.

We remark that the detector and its efficiency response $F_i^\dagger F_i$ do not change with time. What is time dependent is that the detector's efficiency depends on the arrival times of the input signals relative to the detector trigger in a gating window.

3.1.2 *Practical setup for characterization*

Here, we discuss how to test the time-dependent efficiencies of a detector, denoted by $F_i^\dagger F_i$. Suppose that we choose a basis for $F_i^\dagger F_i$ such that its diagonal elements represent the arrival times of the incoming signal. In this basis, the diagonal elements can be tested easily by sending signals into the detector at different times. The separation between two adjacent test times is determined by the bandwidth of the frequency filter as discussed above, and the test pulse shape should ideally be Gaussian with a width also determined by the bandwidth of the filter. The off-diagonal elements can be found by sending in signals in superpositions of the test times with different phases. One possible practical setup to generate superpositions of the test times is shown in Fig. 4. Ideally, one should test the detector using a single-photon

source, since this is consistent with the assumption we use in this paper that Eve always sends single-photon signals to Bob. In principle, the off-diagonal terms may not be zero, since it is conceivable that there exist multiple reflection sites in the detection channel that can give rise to correlations between pulses of different arrival times. However, in practice, we speculate that the multi-reflected signals are much weaker than the original signals, and therefore the off-diagonal terms may be negligible compared to the diagonal terms. It would be interesting for future study to test practical detectors for the existence of this correlation.

4 Security proof for the noiseless case

In this section, we prove the security of the case where Eve does not introduce any bit or phase errors but only intervenes with the auxiliary dimension. Since we assume Alice uses a single-photon source, the initial state prepared by Alice is

$$(|00\rangle + |11\rangle)_{AB}. \quad (6)$$

Eve does not introduce any noise and she simply attaches an extra system T that represents her intervention in the auxiliary dimension, giving

$$\longrightarrow (|00\rangle + |11\rangle)_{AB} \otimes |\gamma\rangle_{TE}. \quad (7)$$

Note that the state in T is in general mixed, and thus is purified with system E in this representation. Now, the state in BT is sent to Bob and he performs the filtering in Eq. (3) to get

$$\begin{aligned} \longrightarrow |\Psi_1\rangle &= F_z [(|00\rangle + |11\rangle)_{AB} \otimes |\gamma\rangle_{TE}] \\ &= |+\rangle_A [|0\rangle_B F_0 |\gamma\rangle_{TE} + |1\rangle_B F_1 |\gamma\rangle_{TE}] + \\ &\quad |-\rangle_A [|0\rangle_B F_0 |\gamma\rangle_{TE} - |1\rangle_B F_1 |\gamma\rangle_{TE}] \end{aligned} \quad (8)$$

where F_i acts on system T . In the actual protocol, after the filtering operation F_z , both Alice and Bob perform measurements on their systems in the Z basis to obtain their raw keys. Bob corrects the bit errors in his raw key according to the error syndromes sent by Alice through a secret classical channel, thus making Alice's and Bob's raw keys the same. After this error correction step, they multiply the same random matrix to their raw keys (for privacy amplification) to arrive at the final secret key. The essence of Koashi's proof [18] is that since the final secret key is derived from Alice's raw key obtained in the Z basis, Alice and Bob's main goal is to guarantee that system A of Alice is in an X eigenstate. In this case, because the uncertainty of system A in the X basis is minimized, by the uncertainty principle, Eve's uncertainty of system A in the Z basis is maximized, and thus the final key is secret to Eve.

Thus, to prove security using Koashi's proof, we consider that Bob performs a virtual measurement on system BT in order to predict Alice's X -basis measurement outcome on system A (see Fig. 5(b)). Essentially, system T (though not carrying bit information) acts as a shield [36] that protects Alice and Bob's key from Eve. Loosely speaking, the uncertainty associated with using Bob's virtual measurement to predict Alice's X -basis measurement outcome is related to Eve's information on the key before privacy amplification. The advantage of using Koashi's proof is that there is no restriction on Bob's virtual measurement on system

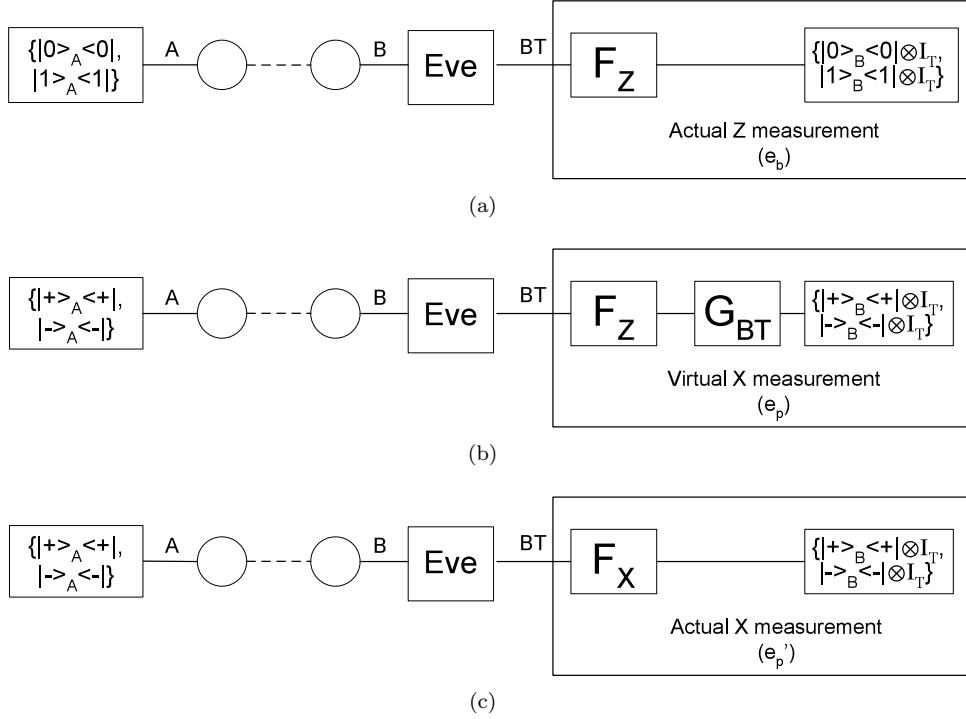


Fig. 5. The top figure shows the actual measurement by Bob to general key bits in the Z -basis, with the corresponding bit error rate of e_b . The middle figure shows the virtual measurement by Bob for helping Alice predict her X -basis measurement outcomes on system A for the key bits generated from Z -basis measurements, with the corresponding (virtual) phase error rate of e_p . The bottom figure shows the actual measurement by Bob in the X -basis, with the corresponding (actual) phase error rate of e'_p .

BT . He is allowed to perform any quantum measurement after the filter F_z . This measurement is not performed in practice and thus whether it is physically realizable is not a concern. The only concern (or restriction) is that we have to make sure that statistics of virtual protocol can be well estimated using those of the actual protocol. Thus, we would like to construct a virtual measurement for Bob aiming at predicting Alice's X -basis measurement outcome with high certainty.

Procrustean method of filtering for Bob's virtual measurement

The objective for Bob is to distinguish the two non-orthogonal states in system BT corresponding to Alice's $|+\rangle$ and $|-\rangle$ states in Eq. (8). The non-orthogonality stems from the efficiency mismatch between the two detectors and this makes the problem more difficult than the perfect-detector case. What complicates the problem even further is that the state Bob tries to measure is not known a priori, owing to the fact that the initial state in system T is unknown. Nevertheless, we propose a simple way to identify the two non-orthogonal states, which is by orthogonalizing them with a filter that may succeed with a probability less than one. The idea of orthogonalizing each signal independently is known as the Procrustean method of filtering [49]. Although our filtering method may not be optimal since we are oper-

ating on individual signals independently, it does provide a simple and intuitive method that magically orthogonalizes the two states even though the initial state in system T is unknown.

In this paper, we specialize in a trick to constructing such a virtual measurement by inverting the filtering operations F_i in Eq. (8) as follows. Bob first performs a filtering

$$G_{BT} = |0_z\rangle_B \langle 0_z| \otimes (CF_0^{-1})_T + |1_z\rangle_B \langle 1_z| \otimes (CF_1^{-1})_T \quad (9)$$

on system BT of Eq. (8) and then performs an X -basis measurement on system B (i.e., with POVM $\{|+\rangle_B \langle +| \otimes \mathbb{I}_T, |-\rangle_B \langle -| \otimes \mathbb{I}_T\}$). Here, we introduce a $d \times d$ matrix C to ensure that G_{BT} is a valid filtering operation (i.e., C is chosen so that $G_{BT}^\dagger G_{BT} \leq \mathbb{I}$). See Appendix B for the derivation of C .

After applying this filter G_{BT} to Eq. (8), the whole state becomes

$$\begin{aligned} &\longrightarrow G_{BT} |\Psi_1\rangle \\ &= [|++\rangle_{AB} + |--\rangle_{AB}] \otimes C |\gamma\rangle_{TE}. \end{aligned} \quad (10)$$

where C acts on system T . The magic of the filter G_{BT} is that even though the initial state of system T is unknown, the filter is still able to concentrate an perfect EPR pair in system AB . Since now there is an EPR pair in system AB , an X -basis measurement outcome on system B is perfectly correlated with an X -basis measurement outcome on system A . Thus, when Bob measures in the X basis on system B of the successfully filtered state in Eq. (10), he is able to predict Alice's X -basis measurement outcome with complete certainty, and this is enough to prove security. Once Alice and Bob know that Alice's state is an X eigenstate, the final key derived from the Z -basis measurements of Alice's state is then secret to Eve. The probability of successful filtering is

$$p_{\text{succ}} = \frac{\text{Tr}[G_{BT} |\Psi_1\rangle \langle \Psi_1| G_{BT}^\dagger]}{\text{Tr}[|\Psi_1\rangle \langle \Psi_1|]} \quad (11)$$

$$= \frac{2 \langle \gamma | (C^\dagger C)_T \otimes I_E |\gamma\rangle_{TE}}{\langle \gamma | (F_0^\dagger F_0 + F_1^\dagger F_1)_T \otimes I_E |\gamma\rangle_{TE}}. \quad (12)$$

Therefore, among all the N qubit pairs shared by Alice and Bob, Bob is able to predict Alice's X -basis measurement outcomes of $N p_{\text{succ}}$ key bits, since he knows whether the virtual filtering on each bit succeeded or not when it is performed. By applying the arguments of Koashi's proof, the secret key generation rate is simply p_{succ} . Since the state $|\gamma\rangle$ in Eq. (12) is chosen by Eve, the worst-case final secret key generation rate on detected signals is

$$R_{\text{noiseless}} = \max_C \min_{|\gamma\rangle} p_{\text{succ}}, \quad (13)$$

which is a lower bound on the key generation rate. The detectors' efficiency matrices $F_0^\dagger F_0$ and $F_1^\dagger F_1$ are assumed to be known. In this case, the final secret key generation rate on detected signals is found by solving Eq. (13) (see Appendix B for detail) and it is equal to

$$R_{\text{noiseless}} = \frac{2}{1 + \max \left(D_1, \frac{1}{D_1}, \dots, D_d, \frac{1}{D_d} \right)} \quad (14)$$

where $D = \text{diag}(D_1, \dots, D_d)$ is a diagonal matrix with positive real elements (which are the eigenvalues) and is determined from the Hermitian decomposition of $F_0(F_1^\dagger F_1)^{-1}F_0^\dagger = UDU^\dagger$. The elements of D represents the ratios of the efficiencies of the two detectors and when the assignment of F_0 and F_1 is reversed, D would also be inverted. If the efficiency matrices F_i are only partially known, one can find the worst-case key generation rate by also minimizing Eq. (13) over them. Throughout the derivation, we have assumed that F_0 and F_1 have full rank (or invertible). Otherwise, we can show that the key generation rate is zero (see below). Thus, characterization of the detectors is very important.

Special case 1: F_i is not invertible

Suppose that F_0 is not invertible (i.e., not full rank) and the nullspace of F_0 and that of F_1 are different^c(F_1 may be invertible). In this case, the worst-case final key generation rate is zero. One may observe this from Eq. (8). Eve may choose $|\gamma\rangle$ to be in the nullspace of F_0 and not in the nullspace of F_1 , leading to system A completely disentangled with system B . Thus, no key can be generated in this case, since entanglement is a precondition for generating secret keys [50].

Special case 2: only diagonal terms are known

Note that if only the diagonal terms of $F_0^\dagger F_0$ and $F_1^\dagger F_1$ are known, the worst-case final key generation rate is zero. Since only the diagonal terms are known, the final key generation rate is determined by minimizing over the off-diagonal terms. One can imagine that the off-diagonal terms are chosen such that F_0 is not invertible and F_1 is invertible. Thus, this case is reduced to special case 1, which allows us to conclude that the final key generation rate in this case is zero.

Special case 3: F_0 and F_1 are diagonal

Here, we consider the special case that the Bob's detectors' responses to the time-shifts, $F_i^\dagger F_i$, $i = 0, 1$, are diagonal, i.e., there is no correlation in the efficiencies between time-shifts. Suppose the efficiency matrices are $F_i^\dagger F_i = \text{diag}(\eta_i(t_1), \eta_i(t_2), \dots)$. We compute the final key generation rate using Eq. (14). Note that $F_0(F_1^\dagger F_1)^{-1}F_0^\dagger = \text{diag}\left(\frac{\eta_0(t_1)}{\eta_1(t_1)}, \frac{\eta_0(t_2)}{\eta_1(t_2)}, \dots\right)$. Using this fact, the final key generation rate on detected signals is

$$R_{\text{noiseless, diag}} = \min_t \frac{2 \min(\eta_0(t), \eta_1(t))}{\eta_0(t) + \eta_1(t)}. \quad (15)$$

5 General security proof

In this section, we prove security under the most general attack by Eve in which she can coherently process the signals sent by Alice and perform a joint measurement on her ancillas. In this general case, Eve's action on the l th bit can be described by her preparing a pure state system T (the auxiliary domain to which the detectors respond) and performing a superoperation on both systems B and T , as follows:

$$|\Psi_2^{(l)}\rangle = \sum_i E_{BT}^{(l,i)}(|00\rangle + |11\rangle)_{AB} \otimes |0\rangle_T \otimes |i\rangle_E \quad (16)$$

^cIf F_0 and F_1 have the same nullspaces, then they can be reduced to two invertible matrices.

where $E_{BT}^{(l,i)}$ is the operation element for the l th bit and it is responsible for introducing bit and phase errors. Note that it can depend on Eve's action on all other bits. Now, the state in BT is sent to Bob and he performs the filtering in Eq. (3) as in the noiseless case to get

$$\longrightarrow F_z |\Psi_2^{(l)}\rangle. \quad (17)$$

As in Fig. 5(b), in order to estimate the amount of privacy amplification, we assume that Bob performs the virtual measurement by applying a filter to $F_z |\Psi_2^{(l)}\rangle$. Bob applies the same filter G_{BT} in Eq. (9) as in the noiseless case and we have

$$\longrightarrow |\Psi_3^{(l)}\rangle = G_{BT} F_z |\Psi_2^{(l)}\rangle. \quad (18)$$

Thus, after Bob measures in the X basis on system B of the successfully filtered state in Eq. (18), he is able to predict Alice's X -basis measurement outcome with uncertainty indicated by the virtual phase error probability of $|\Psi_3^{(l)}\rangle$. On the other hand, the actual phase error probability (e'_p) is not generated by this state; it is generated by some other state, namely $F_x |\Psi_2^{(l)}\rangle$ [Fig. 5(c)]. Thus, we need to estimate the virtual phase error probability (e_p) of the filtered state $|\Psi_3^{(l)}\rangle$ [Fig. 5(b)] from the actual phase error probability (e'_p) [Fig. 5(c)]. In addition, we need to lower bound the probability of successful filtering of the state $F_z |\Psi_2^{(l)}\rangle$. Overall, we are interested in the formulas for the actual bit error probability (e_b) of $F_z |\Psi_2^{(l)}\rangle$, the virtual phase error probability (e_p) of $|\Psi_3^{(l)}\rangle$, the actual phase error probability (e'_p) of $F_x |\Psi_2^{(l)}\rangle$, and the virtual filtering probability ($p_{\text{succ,noisy}}$) of $F_z |\Psi_2^{(l)}\rangle$:

$$e_b = \frac{\sum_l \text{Tr}[P_{\text{bit}} F_z |\Psi_2^{(l)}\rangle \langle \Psi_2^{(l)}| F_z^\dagger]}{\sum_l \langle \Psi_2^{(l)}| F_z^\dagger F_z |\Psi_2^{(l)}\rangle} \quad (19)$$

$$e_p = \frac{\sum_l \text{Tr}[P_{\text{phase}} |\Psi_3^{(l)}\rangle \langle \Psi_3^{(l)}|]}{\sum_l \langle \Psi_3^{(l)}| \Psi_3^{(l)}\rangle} \quad (20)$$

$$e'_p = \frac{\sum_l \text{Tr}[P_{\text{phase}} F_x |\Psi_2^{(l)}\rangle \langle \Psi_2^{(l)}| F_x^\dagger]}{\sum_l \langle \Psi_2^{(l)}| F_x^\dagger F_x |\Psi_2^{(l)}\rangle} \quad (21)$$

$$p_{\text{succ,noisy}} = \frac{\sum_l \langle \Psi_3^{(l)}| \Psi_3^{(l)}\rangle}{\sum_l \langle \Psi_2^{(l)}| F_z^\dagger F_z |\Psi_2^{(l)}\rangle} \quad (22)$$

where $P_{\text{bit}} = |01\rangle_{AB} \langle 01| + |10\rangle_{AB} \langle 10|$ and $P_{\text{phase}} = |+-\rangle_{AB} \langle +-| + |-+\rangle_{AB} \langle -+|$. These quantities are specified by Eve through her selection of the attack strategy $E_{BT}^{(l,i)}$. Although there seems to be many dimensions in the attack strategy (as l runs over all qubit pairs and i over any range), one can simplify the attack into a small number of dimensions when probabilities are concerned.

For the case we consider in this paper, it is shown in Appendix C that the various proba-

bilities of interest in Eqs. (19)-(22) can be simplified with a collective attack to

$$e_b = \frac{\text{Tr}[\rho_E(\tilde{Z}_{10} \otimes F_0^\dagger F_0 + \tilde{Z}_{01} \otimes F_1^\dagger F_1)]}{\text{Tr}[\rho_E((\tilde{Z}_{00} + \tilde{Z}_{10}) \otimes F_0^\dagger F_0 + (\tilde{Z}_{11} + \tilde{Z}_{01}) \otimes F_1^\dagger F_1)]} \quad (23)$$

$$e_p = \frac{\text{Tr}[\rho_E(\tilde{X}_{-+} + \tilde{X}_{+-}) \otimes C^\dagger C]}{\text{Tr}[\rho_E(\tilde{X}_{++} + \tilde{X}_{-+} + \tilde{X}_{+-} + \tilde{X}_{--}) \otimes C^\dagger C]} \quad (24)$$

$$e'_p = \frac{\text{Tr}[\rho_E(\tilde{X}_{-+} \otimes F_0^\dagger F_0 + \tilde{X}_{+-} \otimes F_1^\dagger F_1)]}{\text{Tr}[\rho_E((\tilde{X}_{++} + \tilde{X}_{-+}) \otimes F_0^\dagger F_0 + (\tilde{X}_{--} + \tilde{X}_{+-}) \otimes F_1^\dagger F_1)]} \quad (25)$$

$$p_{\text{succ, noisy}} = \frac{\text{Tr}[\rho_E((\tilde{Z}_{00} + \tilde{Z}_{10} + \tilde{Z}_{11} + \tilde{Z}_{01}) \otimes C^\dagger C)]}{\text{Tr}[\rho_E((\tilde{Z}_{00} + \tilde{Z}_{10}) \otimes F_0^\dagger F_0 + (\tilde{Z}_{11} + \tilde{Z}_{01}) \otimes F_1^\dagger F_1)]} \quad (26)$$

where ρ_E represents Eve's action, which is averaged over all signals, and has dimensions $4d \times 4d$ (again, $d \times d$ are the dimensions of F_i and C) and C is from Eq. (B.16). Here, $\tilde{Z}_{i,j}$ and $\tilde{X}_{i,j}$ are constant 4×4 matrices given in Eq. (C.11). [Note that we are using C determined in the noiseless case. However, it can be shown (in a similar fashion as in the noiseless case) that the same C is obtained if we maximize the filtering probability $p_{\text{succ, noisy}}$ over C (which is related to problem (P1') in Section 5.2).]

It is worth noting that the security proofs for a three-state protocol [51] and the SARG04 protocol [52, 53] that share the same technique (the Azuma's inequality [54]) as the current paper reduce to collective attacks in a more straightforward manner. In their cases, the normalizations of all probabilities of interest (the bit and phase error probabilities) are the same and this together with the concavity of the relations between the probabilities immediately reduce joint attacks to collective attacks. In the case of the current paper, the normalizations (i.e., the denominators of Eqs. (19)-(22)) are different; and thus we need a more involved analysis to reduce to collective attacks.

We remark that in our general method, we use the Procrustean Method and the trick of inverting the detection efficiency filters when constructing the virtual filter. It is well-known (e.g. Ref. [49]) that in entanglement distillation theory the Procrustean Method is, in general, sub-optimal. On the other hand, our method, despite its sub-optimality, provides an instructive and easily understandable way to prove security.

5.1 *Bounding filtering probability $p_{\text{succ, noisy}}$ and phase error probability e_p*

Both the virtual filtering probability ($p_{\text{succ, noisy}}$) and virtual phase error probability (e_p) ultimately determine the key generation rate (cf. Eq. (31)). Thus, we bound them by numerically optimizing them over Eve's action subject to the observed bit and phase error rates. One important tool that we rely on to identify the the observed rates with the corresponding probabilities is the Azuma's inequality [54], which asserts that the sum of the probabilities for an event over all trials is asymptotically close to the observed count of the event (this inequality was similarly used in other security proofs [51–53, 55, 56]).^d Thus, the rate of successful virtual

^d In order to see how the Azuma's inequality is applied to Eqs. (19)-(22), consider e_b in Eq. (19) as a concrete example. We apply the Azuma's inequality to the numerator and denominator separately. The numerator in the right hand side of Eq. (19) is $\text{Pr}\{\text{bit error and conclusive result}\}$ and the denominator is $\text{Pr}\{\text{conclusive result}\}$. Since e_b is defined as the bit error rate *conditional on* conclusive bits, we can apply the Azuma's inequality to the numerator of Eq. (19) to get the actual number of bits with error and apply the Azuma's inequality to the denominator to get the actual number of conclusive bits. Dividing these two numbers gives us e_b .

filtering can be lower bounded as

$$\begin{aligned} & \text{minimize } p_{\text{succ, noisy}} \\ & \text{subject to } e_b = \text{observed } e_b \\ & \quad e'_p = \text{observed } e'_p \end{aligned} \tag{P1}$$

and the virtual phase error rate can be upper bounded as

$$\begin{aligned} & \text{maximize } e_p \\ & \text{subject to } e_b = \text{observed } e_b \\ & \quad e'_p = \text{observed } e'_p \end{aligned} \tag{P2}$$

where the optimization is over Eve's action ρ_E and the formulas for the error probabilities and the filtering probability are from Eqs. (23)-(26). Note that both problems (P1) and (P2) can be expressed as a polynomial problem by multiplying the denominator of each fraction in each of the constraints; and thus the two problems can be solved numerically and efficiently^e[57,58].

When $e_b = e'_p = 0$, solving these two problems gives the same noiseless-case result in Eq. (14).

When $F_0 = F_1$ (meaning that there is no efficiency mismatch), it can easily be checked that $p_{\text{succ, noisy}} = 1$ and $e_p = e'_p$, as expected.

We remark that although both problems (P1) and (P2) involve only the average error rates, improvement in the bounds may be obtained by, for example, separating the error rates for bits "0" and "1".

5.2 Suboptimal bounds

In order to better understand the relationship between the efficiency mismatch and the phase error probability e_p or the filtering probability $p_{\text{succ, noisy}}$, we compute suboptimal bounds for these two quantities. These bounds are obtained by simply dropping the constraints in problems (P1) and (P2). Specifically, we solve

$$\text{minimize } p_{\text{succ, noisy}} \tag{P1'}$$

and

$$\text{maximize } \frac{e_p}{e'_p} \tag{P2'}$$

where the optimization is over Eve's action ρ_E and the formulas for the error probabilities and the filtering probability are from Eqs. (23)-(26). Solving these problems gives (see Appendix D for detail)

$$p_{\text{succ, noisy}} \geq \min \left(D_1, \frac{1}{D_1}, \dots, D_d, \frac{1}{D_d} \right) \tag{27}$$

$$\frac{e_p}{e'_p} \leq \max \left(D_1, \frac{1}{D_1}, \dots, D_d, \frac{1}{D_d} \right) \tag{28}$$

^eIt seems that considering rank-one ρ_E is always sufficient to achieve the optimal solution based on our simulation results. However, we have not been able to prove this. Note that convexity/concavity of (P1)/(P2) does not immediately give rise to this conclusion.

where $D = \text{diag}(D_1, \dots, D_d)$ is a diagonal matrix with positive real elements and is determined from the Hermitian decomposition of $F_0(F_1^\dagger F_1)^{-1}F_0^\dagger = UDU^\dagger$. In other words, the virtual filtering probability and the virtual phase error probability are related to the minimum and maximum efficiency ratios between the two detectors. Note that the right hand side of Eq. (27) is the inverse of that of Eq. (28).

5.3 Key generation rate

After the virtual filtering operation, Bob can predict Alice's X -basis measurement outcomes with an error probability of e_p for $Np_{\text{succ, noisy}}$ key bits. In light of Koashi's proof, Bob's prediction removes some uncertainty on Alice's X -basis measurement outcomes (through Bob's communication to Alice). The remaining uncertainty can be removed (with high probability) by Alice performing hashing on the key bits in m rounds, where m is less than N in general. In our case, $m = (N - Np_{\text{succ, noisy}}) + Np_{\text{succ, noisy}}H_2(e_p)$ where the first (second) part represents the key bits for which Bob's virtual filter did not (did) succeed. Here, $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy function. According to the proof, the number of secure key bits generated is (without error correction)

$$\begin{aligned} K_{\text{PA}} &= N - m \\ &= Np_{\text{succ, noisy}}(1 - H_2(e_p)). \end{aligned} \quad (29)$$

The amount of (pre-shared) secret key bits sacrificed for error correction using encrypted one-way communication is

$$K_{\text{EC}} = NH_2(e_b). \quad (30)$$

Combining them gives the final key generation rate on detected signals:

$$\begin{aligned} R_{\text{noisy}} &= [K_{\text{PA}} - K_{\text{EC}}]/N \\ &= p_{\text{succ, noisy}}(1 - H_2(e_p)) - H_2(e_b) \end{aligned} \quad (31)$$

where $p_{\text{succ, noisy}}$ and e_p are obtained by solving problems (P1) and (P2), respectively. Alternatively, they may be obtained from the suboptimal bounds in Eqs. (27) and (28). Also, it is worth noting that we do not need to separately bound $p_{\text{succ, noisy}}$ and e_p with two separate optimization problems. We can instead minimize the key generation rate in Eq. (31) subject to the observed error rates (which are the common constraints of (P1) and (P2)). However, this problem is not a convex optimization problem (due to the nonlinear equality constraints) or a polynomial optimization problem (due to the non-polynomial objective function) and thus may not easily be solved optimally and efficiently.

5.4 Example 1: scalar efficiencies

Consider a QKD system in which the two detectors have constant but different efficiencies. This means that the detection efficiency matrices, $F_i^\dagger F_i, i = 0, 1$, are scalar. In this case, one can easily compute the noiseless key generation rate on detected signals by using Eq. (14) or Eq. (15) to be

$$R_{\text{noiseless, scalar}} = \frac{2 \min(\eta_0, \eta_1)}{\eta_0 + \eta_1}, \quad (32)$$

where $\eta_i = F_i^\dagger F_i$. On the other hand, this formula for the scalar efficiency case can be obtained by the following simple argument. Bob can artificially make the efficiencies of the two detectors the same by randomly discarding some detection events of the detector with the higher efficiency in the data postprocessing step. To arrive at the above formula, suppose that Alice sends N signals (with equal numbers of bits “0” and “1”) to Bob. Then, Bob will detect $\frac{N}{2}\eta_0$ number of “0”s and $\frac{N}{2}\eta_1$ number of “1”s, giving the total number of detected signals $\frac{N}{2}(\eta_0 + \eta_1)$. Now, assuming that $\eta_0 < \eta_1$, Bob discards some of detection events of the detector corresponding to bit “1”, so that effectively $\frac{N}{2}\eta_0$ number of “0”s and $\frac{N}{2}\eta_0$ number of “1”s are retained to form the final key (there is no error correction or privacy amplification since there is no noise). Thus, the final key length is $N\eta_0$, and dividing this by the total number of detected signals gives Eq. (32).

Now, let’s consider the noisy case. The above simple argument with data discarding can also handle the noisy case. After the artificial equalization of the two detection efficiencies, the situation Alice and Bob are facing becomes that considered in Shor-Preskill [7]. This can be seen as follows. When the efficiencies are scalar, Bob’s actual measurement in the W -basis ($W = X, Z$) is described by the filtering operation F_w in Eqs. (3)-(4) (which is a diagonal matrix in the W -basis and represents the efficiency mismatch) followed by the standard W -basis measurement. Now, the artificial equalization can be described by another filter \hat{F}_w which is diagonal in the W -basis such that $F_w \hat{F}_w = cI$ where c is a constant independent of the basis W , meaning that data discarding removes the efficiency mismatch in both bases while incurring some loss. Essentially, this is the same situation as Shor-Preskill’s with a basis-independent loss, and thus their key rate formula can be applied. Taking into account of the loss, the key generation rate for the data-discarding argument is

$$R_{\text{noisy, scalar, discarding}} = \frac{2 \min(\eta_0, \eta_1)}{\eta_0 + \eta_1} (1 - H_2(e_p) - H_2(e_b)). \quad (33)$$

Here, e_b and e_p are the error rates after the data-discarding process corresponding to the Z -basis and X -basis measurement outcomes, respectively. Also, the standard squash model for BB84 [17, 59, 60] can be applied here to handle threshold detectors so that the incoming signals can always be treated as qubits and dark counts as random qubits. This data-discarding argument in conjunction with the Shor-Preskill’s proof bears similarity with our formulation. In fact, the equalization filter \hat{F}_x for the X -basis is the same as the virtual filter G_{BT} in Eq. (9) in our formulation. In our formulation, we assume that this virtual filter G_{BT} is not and/or cannot be performed in practice and therefore we estimate the virtual phase error rate e_p from the actual phase error rate e'_p through problem (P2). On the other hand, with the data-discarding argument, this virtual filter is *actually* performed through the data-discarding process. Thus, one can actually measure the “virtual” phase error rate e_p directly (cf. Fig. 5(b)) without solving problem (P2). This means that our estimation of the virtual phase error rate e_p may be sub-optimal, and, in contrast, the data-discarding protocol allows us to obtain it directly and accurately. Therefore, the data-discarding protocol may give us a higher key generation rate than our general method. A similar argument goes for the successful filtering probability $p_{\text{succ, noisy}}$. This quantity can also be obtained without solving problem (P1) since the virtual filter G_{BT} is actually performed. On the other hand, an analogous argument does not apply to the bit error rate since, in our formulation, no filtering is applied to the states to be measured in the Z basis, whereas, in the data-discarding argument, the

data-discarding filter \hat{F}_z is applied. In summary, the difference between our formulation and the data-discarding argument is that we assume that the virtual filter is not performed in practice. By actually performing the filter, the data-discarding argument avoids solving problems (P1) and (P2). Nevertheless, one may proceed to solve problems (P1) and (P2) with an addition constraint that Eve's attack is symmetric between bits "0" and "1" in both bases to obtain $e_p = e'_p$ and $p_{\text{succ, noisy}} = \frac{2 \min(\eta_0, \eta_1)}{\eta_0 + \eta_1}$. Using these results, our formulation in Eq. (31) gives the key generation rate

$$R_{\text{noisy, scalar}} = \frac{2 \min(\eta_0, \eta_1)}{\eta_0 + \eta_1} (1 - H_2(e_p)) - H_2(e_b). \quad (34)$$

Note that the bit error rate e_b here corresponds to that before data discarding. By comparing Eqs. (33) and (34), we can see that the data-discarding argument gives a higher key generation rate than our general technique when the bit error rate remains the same before and after data discarding. Nevertheless, this simple data-discarding argument does not extend to the general case with non-scalar efficiency matrices, whereas our general technique can handle this general case.

5.5 *Example 2: two-dimensional efficiency matrices*

In this example, we illustrate the application of our proof to the non-trivial case with non-scalar efficiency matrices. Suppose that we have a polarization-coding QKD system in which the two detectors have imperfect efficiency responses to the arrival times of signals (assuming that only two arrival times are allowed for simplicity). The two detectors have the following detection efficiency matrices:

$$F_0^\dagger F_0 = \begin{bmatrix} .8 & -.2 \\ -.2 & .4 \end{bmatrix}, \quad F_1^\dagger F_1 = \begin{bmatrix} .3 & .1 \\ .1 & .9 \end{bmatrix}. \quad (35)$$

Here, the basis used to represent these matrices is the arrival times. Thus, for example, the first detector responds with 80% efficiency when hit by a signal arriving at the first time instant. Also, the fact that the matrices are non-diagonal means that the detectors have non-trivial efficiency responses to signals entangled across the two time instants.

We first compute the efficiency ratios between the two detectors, based on the above two matrices. These ratios are the diagonal elements of the diagonal matrix D which appear in the key generation rate expressions of Eq. (14) and Eq. (31). The ratios are the eigenvalues of $F_0^\dagger F_0 (F_1^\dagger F_1)^{-1}$ and are computed to be

$$D_1 = 3.03, \quad D_2 = 0.356. \quad (36)$$

To get the key generation rate in the noiseless case, we substitute D into Eq. (14) and get

$$R_{\text{noiseless}} = 0.496. \quad (37)$$

To get the key generation rate for the general noisy case, we first compute the C matrix from Eq. (B.16):

$$C = \begin{bmatrix} 0.51 & -0.17 \\ 0.12 & 0.56 \end{bmatrix}. \quad (38)$$

We then use C in the expressions for the various probabilities in Eqs. (23)-(26) and numerically solve for $p_{\text{succ, noisy}}$ and e_p in problems (P1) and (P2) for some given observed error rates. Alternatively, one may determine suboptimal values of $p_{\text{succ, noisy}}$ and e_p using Eqs. (27) and (28) without computing C . Finally, the key generation rate is computed using Eq. (31). The key generation rate for the noisy case with the assumption of $e_b = e'_p$ is plotted in Fig. 6 along with the corresponding filtering probability and phase error rate. Note that the minimum efficiency ratio is $1/D_1 = 0.330$ and the maximum is $D_1 = 3.03$. These are shown as the dashed curve of Fig. 6(a) and the slope of the dashed curve of Fig. 6(b), respectively. Even though the mismatch ratio is quite high, positive key generation rate can still be obtained.

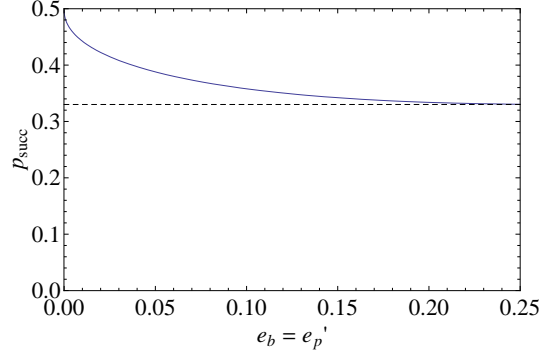
6 Detection scheme with four phase settings

In this section, we prove how randomly switching the bit assignments of the two detectors for each quantum signal can completely eliminate the effect of detection efficiency mismatch. Previously, a four-phase modulation scheme was proposed [31,32] to implement the BB84 protocol with only one detector at Bob's side. This scheme uses only one detector to measure both bit "0" and bit "1". Essentially, an additional bit flip operation is performed at random to prepare the detector for detecting bit "0" or bit "1". So, half of the time, the detector is used for detecting bit "0" and the other half bit "1". To implement this method in a phase-coding BB84 QKD system, Bob's phase modulator applies four phase settings $\{0, \pi/2, \pi, 3\pi/2\}$ instead of the two $\{0, \pi/2\}$ in the normal case. The motivation of the original proposals [31,32] for this scheme was to save one detector but not for security purpose. In fact, since only one detector is used in this scheme, there is no issue of efficiency mismatch between detectors; however, half the bits are lost, lowering the overall efficiency. Moreover, we first pointed out [27] that the efficiency loophole could be closed by incorporating the four phase settings in BB84 even with two detectors. Here, we rigorously prove this claim. Furthermore, we remark that the four-phase scheme can also be used to solve the detection efficiency mismatch problem that arises due to dead-times. In the following, we consider using two detectors together with the four phase settings in BB84. In this case, the overall efficiency is not affected because two detectors are used instead of one. The four phase settings are applied at Bob's side to "average out" the effect of the efficiency responses of the two detectors (see Fig. 7). At first sight, the key generation rate of this scheme may appear to be the average of the rates when Bob performs the bit flip operation and when he does not. This is because if one considers entanglement distillation, the total entanglement available should just be the sum of the entanglement of the two cases. However, when we are concerned with key generations, Bob's action on whether to flip or not is not known to Eve and thus serves to disentangle Eve further (i.e., it acts as a shield [36]). This allows the overall key generation rate to be higher than the average of the two cases. In what follows, we show that indeed this scheme is capable of completely removing the effect of efficiency mismatch and the key generation rate for the no-mismatch case is recovered.

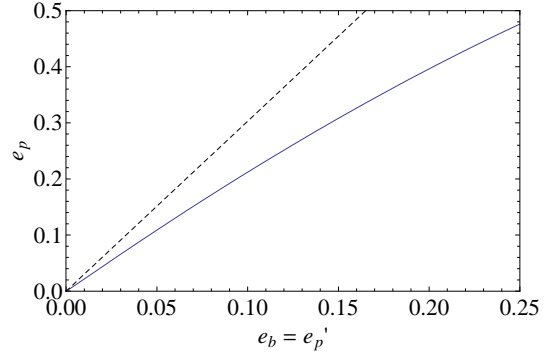
To begin, let's consider that Bob has a quantum coin that determines whether to apply a bit flip operation (which is the same as switching the two detectors). The filtering operations F'_z and F'_x associated with the detectors' responses are (see Fig. 5)

$$F'_z = F_z \otimes |0\rangle_C \langle 0| + X_B F_z X_B \otimes |1\rangle_C \langle 1| \quad (39)$$

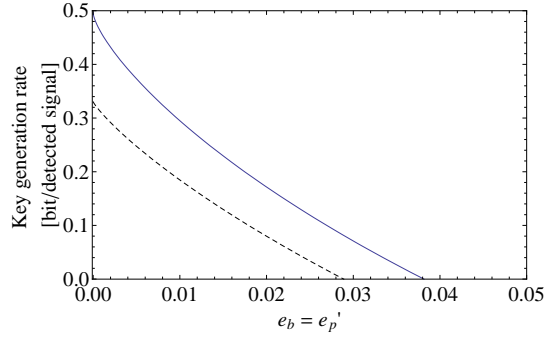
$$F'_x = F_x \otimes |0\rangle_C \langle 0| + Z_B F_x Z_B \otimes |1\rangle_C \langle 1| \quad (40)$$



(a) Probability of successful filtering.



(b) Phase error rate.



(c) Key generation rate.

Fig. 6. Efficiency mismatch example for two-dimensional efficiency matrices. Solid curves are obtained from solving problems (P1) and (P2). Dashed curves are obtained from the suboptimal bounds in Eqs. (27) and (28). The key generation rate is computed using Eq. (31). The maximum efficiency mismatch ratio is $D_1 = 3.03$.

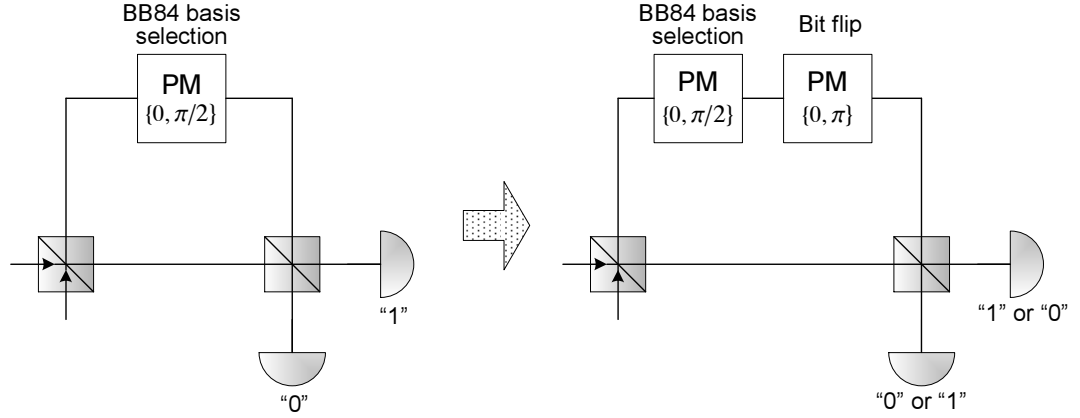


Fig. 7. The diagram on the left is the standard implementation of phase-encoding BB84 with a Mach-Zehner interferometer at Bob's side. Bob selects the measurement basis with a phase modulator set to either 0 or $\pi/2$. The diagram on the right is the four-phase scheme where Bob randomly flips the bit value assignment of the two detectors with a phase modulator. The two logical phase modulators can be implemented as one with four possible phases.

where system C represents the quantum coin, F_z is from Eq. (3), and F_x is from Eq. (4). The entire state after Eve's operation is [cf. Eq. (C.1), which does not involve the quantum coin]

$$|\Psi_4^{(l)}\rangle = \sum_{i,j} E_B^{(l,i,j)} (|00\rangle + |11\rangle)_{AB} \otimes (|0\rangle + |1\rangle)_C \otimes |\gamma(l,i,j)\rangle_T \otimes |i\rangle_E, \quad (41)$$

where $E_B^{(l,i,j)}$ is defined in Appendix C. We design the virtual filter $G_{BT,4\text{-phase}}$ so that the resulting state $G_{BT,4\text{-phase}} F'_z |\Psi_4^{(l)}\rangle$ [Fig. 5(b)] is the same as the state used to determine the actual phase error probability $F'_x |\Psi_4^{(l)}\rangle$ [Fig. 5(c)]. In this way, the virtual X -basis measurement and the actual X -basis measurement exhibit the same phase error probabilities.

The state from which the actual phase error rate is estimated is the state in Eq. (41) filtered with F'_x (see Fig. 5(c)):

$$\begin{aligned} & F'_x |\Psi_4^{(l)}\rangle \\ = & \sum_{i,j} \left\{ \left[\frac{a_I + a_X}{\sqrt{2}} |++\rangle_{AB} + \frac{a_Z - a_Y}{\sqrt{2}} |--\rangle_{AB} \right] \otimes (|0\rangle_C F_0 |\gamma\rangle_T + |1\rangle_C F_1 |\gamma\rangle_T) \right. \\ & + \left. \left[\frac{a_I - a_X}{\sqrt{2}} |--\rangle_{AB} + \frac{a_Z + a_Y}{\sqrt{2}} |+-\rangle_{AB} \right] \otimes (|0\rangle_C F_1 |\gamma\rangle_T + |1\rangle_C F_0 |\gamma\rangle_T) \right\} \otimes |i\rangle_E \end{aligned} \quad (42)$$

where $|\gamma\rangle_T = |\gamma(l,i,j)\rangle_T$ and $a_W = a_W^{(l,i,j)}$, $W = \{I, X, Y, Z\}$ for simplified notation. Now, we design $G_{BT,4\text{-phase}}$ so that $G_{BT,4\text{-phase}} F'_z |\Psi_4^{(l)}\rangle$ is the same as Eq. (42). Notice that

$$\begin{aligned} & F'_z |\Psi_4^{(l)}\rangle \\ = & \sum_{i,j} \left\{ \left[\frac{a_I + a_Z}{\sqrt{2}} |00\rangle_{AB} + \frac{a_X + a_Y}{\sqrt{2}} |10\rangle_{AB} \right] \otimes (|0\rangle_C F_0 |\gamma\rangle_T + |1\rangle_C F_1 |\gamma\rangle_T) \right. \\ & + \left. \left[\frac{a_I - a_Z}{\sqrt{2}} |11\rangle_{AB} + \frac{a_X - a_Y}{\sqrt{2}} |01\rangle_{AB} \right] \otimes (|0\rangle_C F_1 |\gamma\rangle_T + |1\rangle_C F_0 |\gamma\rangle_T) \right\} \otimes |i\rangle_E. \end{aligned} \quad (43)$$

We heuristically design $G_{BT,4\text{-phase}} = U_2 U_1$ in two steps. First, we choose

$$U_1 = |0\rangle_B \langle 0| \otimes I_C \otimes I_T + |1\rangle_B \langle 1| \otimes X_C \otimes I_T \quad (44)$$

which is basically a CNOT operation in system BC . This operation leads to

$$\begin{aligned} & U_1 F'_z |\Psi_4^{(l)}\rangle \\ &= \sum_{i,j} E_B^{(l,i,j)} (|00\rangle + |11\rangle)_{AB} \otimes \left(|0\rangle_C \otimes F_0 |\gamma(l,i,j)\rangle_T + |1\rangle_C \otimes F_1 |\gamma(l,i,j)\rangle_T \right) \otimes |i\rangle_E. \end{aligned} \quad (45)$$

Notice the similarity of Eq. (45) to Eq. (41) which represents the state before the detectors' responses are applied. As a special case when there is no noise (i.e., $E_B^{(l,i,j)} = I$), Eq. (45) becomes the perfect EPR pair in system AB tensor with system CTE , meaning that applying the virtual filter U_1 is already sufficient to completely eliminate the effect of detection efficiency mismatch. In this special case, the probability of successful virtual filtering is 1 (since U_1 is unitary) and thus the key generation rate on detected signals is 1.

Let's continue to design U_2 , which is needed for the noisy case. By choosing

$$U_2 = |+\rangle_B \langle +| \otimes I_C \otimes I_T + |-\rangle_B \langle -| \otimes X_C \otimes I_T, \quad (46)$$

one can easily verify that $U_2 U_1 F'_z |\Psi_4^{(l)}\rangle = F'_x |\Psi_4^{(l)}\rangle$. Thus, the final virtual filter is $G_{BT,4\text{-phase}} = U_2 U_1$. Note that $G_{BT,4\text{-phase}}$ is not $F'_x F_z'^{-1}$ in general (i.e., we did not invert the filters in a naive way). To find the final key generation rate on detected signals, we may use Eq. (31) with the probability of successful virtual filtering $p_{\text{succ,noisy}} = 1$ (since $G_{BT,4\text{-phase}}$ is unitary) to get

$$R_{4\text{-phase}} = 1 - H_2(e_p) - H_2(e_b) \quad (47)$$

where e_p is the phase error rate estimated using the actual X -basis measurement (see Fig. 5(c)) and e_b is the bit error rate estimated using the actual Z -basis measurement (see Fig. 5(a)). Apparently, this key generation rate in Eq. (47) is the same as if there is no efficiency mismatch (e.g., Refs. [7,61]). This means that the effect of the efficiency mismatch is completely removed by using this four-state scheme.

7 Multi-photon signals

In practice, the channel may receive multi-photon signals from Alice and may emit multi-photon signals to Bob. We discuss this issue here.

7.1 Input with multi-photon signals

Since our detector model and proof work on the assumption that the input to Bob are single-photon signals, applying our proof to practice settings where multi-photon signals may be present requires special attention. In order to cope with this practical issue, one may consider implementing the detector-decoy idea of Ref. [62] to estimate the fraction of single-photon input to Bob. The detector-decoy idea involves the receiver Bob adding an attenuator in front of his detector to monitor the transmission properties (e.g., transmittance and quantum bit error rate) as a function of attenuation. By solving linear equations related to these properties,

one can infer the fraction of single-photon input to Bob. Signals received by Bob are randomly chosen to be used for this estimation process or the normal key generation process. Upon knowing the fraction of single-photon input signals, one can apply the tagged-signals idea of [17] to compute the overall key generation rate by assuming that all multi-photon input signals are insecure and only single-photon input signals are distillable. Our proof provides a way to compute the number of secure bits in the single-photon parts, and this is what is needed when we apply [17] to extend the situation with multi-photon input signals. When applying our proof in this case, one may also assume pessimistically that all errors come from the single-photon parts. Note that when applying the idea of [17], we only need to know the fraction of the single-photon input signals but not their positions.

7.2 Phase-randomized weak coherent source

Our proof can also be applied to the case with a phase-randomized weak coherent source, with or without decoy states [63–70], by following the argument in [17]. Essentially, to incorporate both multi-photon inputs and outputs, one estimates the fraction of single-photon input signals that originated from single-photon outputs, and applies the result of [17].

8 Concluding remark

In practice, it is hard to build two identical detectors. Owing to widespread existence of detector dead-times or different detector responses as functions of some auxiliary variables in, for example, time, frequency or spatial domain, two detectors almost certainly exhibit detection efficiency mismatch. For practical QKD systems to be secure, it is thus important to prove the security of QKD systems with detection efficiency mismatch. In this paper, we prove the security of the BB84 protocol when the detectors respond to some auxiliary domain, in addition to the qubit space representing the information bit in the normal case. Specifically, we show that once the detectors' responses to the auxiliary domain (F_i) are characterized, we can obtain an amount of privacy amplification sufficient to remove Eve's information on the final key. We show that this amount is directly related to the maximum efficiency ratio between the two detectors.

We show that the detectors' responses F_i can be characterized with a finite number of samples even when time is the auxiliary domain by using a narrow-band frequency filter. Thus, we may test F_i with a finite number of test signals in practice in order to characterize it. One issue about the applicability of our proof is that we assume that the detectors' responses F_i are stable over time. Once we have stable estimates of F_i from testing the detectors, our proof can be applied to obtain the final key generation rate.

The key generation rate derived in this paper may not be optimal and there may be ways to improve it. Our speculation is based on two observations: one in the noiseless case and another in the noisy case. For the first observation in the noiseless case, suppose that the two detectors have different scalar efficiencies, i.e. $F_i = \eta_i$. In this case, the state shared by Alice and Bob is $\sqrt{\eta_0}|00\rangle + \sqrt{\eta_1}|11\rangle$. Since there are $2^{N h_2(\eta_0/(\eta_0+\eta_1))}$ typical strings, the key generation rate is simply $h_2(\eta_0/(\eta_0 + \eta_1))$, which may be obtained by applying the appropriate amount of privacy amplification (see also [49]). On the other hand, our current proof yields a key generation rate of $2 \min(\eta_0, \eta_1)/(\eta_0 + \eta_1)$ (see Eq. (15)), which is in general smaller. For the second observation in the noisy case, we see in Example 1 (see Sec. 5.4) that

a simple data-discarding argument can produce a higher key generation rate than our proof (when having scalar efficiencies). Thus, we speculate that there may be ways to improve the key generation rate even in the general noisy case where non-scalar detection efficiencies F_i are used. The source of sub-optimality of our current proof may be that we distinguish non-orthogonal states on Bob's side on each signal independently. Thus, it would be interesting to apply a collective method for entanglement concentration, instead of the Procrustean method for entanglement concentration, to the context of QKD. We leave this potential improvement for future work.

We have shown rigorously that using four phase settings in BB84 can equalize the detection efficiencies for bits “0” and “1”, thus solving the detection efficiency mismatch problem. However, as noted in our introduction, Eve may try to break this four-state-measurement counter-measure by using a combined strong pulse attack and time-shift attack [30,34]. This demonstrates that counter-measures may lead to new attacks.

Acknowledgments

We thank J.-C. Boileau and D. Gottesman for enlightening discussions. Support of the funding agencies CFI, CIPI, the CRC program, CIFAR, MITACS, NSERC, QuantumWorks, OIT, and PREA is gratefully acknowledged. C.-H. F. Fung gratefully acknowledges support from the Postdoctoral Fellowship program of NSERC of Canada and the RGC grant No. HKU 701007P of the HKSAR Government.

References

1. C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in *Proc. of IEEE Int. Conference on Computers, Systems, and Signal Processing*, IEEE Press, New York, Dec. 1984, pp. 175–179.
2. A. K. Ekert (1991), *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., vol. 67, pp. 661–663.
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden (2002), *Quantum cryptography*, Rev. Mod. Phys., vol. 74, pp. 145–195.
4. D. Mayers (2001), *Unconditional security in quantum cryptography*, J. of ACM, vol. 48, pp. 351–406, preliminary version in Mayers, D. Advances in Cryptology-Proc. Crypto '96, vol. 1109 of Lecture Notes in Computer Science, Koblitz, N. Ed. (Springer-Verlag, New York, 1996), pp. 343–357.
5. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, *A proof of the security of quantum key distribution*, in *Proc. of the thirty-second annual ACM symposium on Theory of computing*, ACM Press, New York, 2000, pp. 715–724.
6. H.-K. Lo and H. F. Chau (1999), *Unconditional security of quantum key distribution over arbitrarily long distances*, Science, vol. 283, pp. 2050–2056.
7. P. W. Shor and J. Preskill (2000), *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett., vol. 85, pp. 441–444.
8. M. Ben-Or (2002), *Security of quantum key distribution protocols*, presentation at MSRI 2002, available at <http://www.msri.org/publications/ln/msri/2002/quantumintro/ben-or/1/index.html>.
9. M. Koashi and J. Preskill (2003), *Secure quantum key distribution with an uncharacterized source*, Phys. Rev. Lett., vol. 90, p. 057902.
10. R. Renner, N. Gisin, and B. Kraus (2005), *Information-theoretic security proof for quantum-key-distribution protocols*, Phys. Rev. A, vol. 72, p. 012332.

11. R. Renner and R. König, *Universally composable privacy amplification against quantum adversaries*, in *Proc. of the Second Theory of Cryptography Conference (TCC) 2005, Lecture Notes in Computer Science*, vol. 3378, Springer, Berlin, 2005, pp. 407–425.
12. B. Kraus, N. Gisin, and R. Renner (2005), *Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication*, *Phys. Rev. Lett.*, vol. 95, p. 080501.
13. D. Gottesman and H.-K. Lo (2003), *Proof of security of quantum key distribution with two-way classical communications*, *IEEE Trans. Inform. Theory*, vol. 49, pp. 457–475.
14. H. F. Chau (2002), *Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate*, *Phys. Rev. A*, vol. 66, p. 060302(R).
15. M. Christandl, R. Renner, and A. Ekert (2004), *A generic security proof for quantum key distribution*, {e-print}arXiv:quant-ph/0402131.
16. H. Inamori, N. Lütkenhaus, and D. Mayers (2001), *Unconditional security of practical quantum key distribution*, {e-print}arXiv:quant-ph/0107017.
17. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill (2004), *Security of quantum key distribution with imperfect devices*, *Quantum Information and Computation*, vol. 5, pp. 325–360.
18. M. Koashi (2006), *Unconditional security proof of quantum key distribution and the uncertainty principle*, *J. Phys. Conf. Ser.*, vol. 36, p. 98, {e-print}arXiv:quant-ph/0505108.
19. M. Koashi (2006), *Efficient quantum key distribution with practical sources and detectors*, {e-print}arXiv:quant-ph/0609180.
20. B. Kraus, C. Branciard, and R. Renner (2007), *Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses*, *Phys. Rev. A*, vol. 75, p. 012316.
21. M. Hayashi (2007), *General theory for decoy-state quantum key distribution with arbitrary number of intensities*, {e-print}arXiv:quant-ph/0702251.
22. H.-K. Lo and J. Preskill (2007), *Security of quantum key distribution using weak coherent states with nonrandom phases*, *Quantum Information and Computation*, vol. 7, pp. 431–458.
23. T. Marshall, E. Santos, and F. Selleri (1983), *Local realism has not been refuted by atomic cascade experiments*, *Phys. Lett. A.*, vol. 98, pp. 5–9.
24. M. Ferrero, T. W. Marshall, and E. Santos (1990), *Bell's theorem: Local realism versus quantum mechanics*, *Am. J. Phys.*, vol. 58, pp. 683–688.
25. V. Makarov, A. Anisimov, and J. Skaar (2006), *Effects of detector efficiency mismatch on security of quantum cryptosystems*, *Phys. Rev. A*, vol. 74, p. 022313.
26. V. Makarov and J. Skaar (2007), *Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols*, {e-print}arXiv:quant-ph/0702262.
27. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma (2007), *Time-shift attack in practical quantum cryptosystems*, *Quantum Information and Computation*, vol. 7, pp. 73–82.
28. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo (2007), *Experimental demonstration of time-shift attack against practical quantum key distribution systems*, {e-print}arXiv:0704.3253[quant-ph].
29. A. Ghatak and K. Thyagarajan, *An Introduction to Fiber Optics*. Cambridge, UK: Cambridge University Press, 1998, ch. 15.5 and 16.5.
30. H.-K. Lo (2007), *Experimental time-shift attack against practical quantum key distribution (QKD) systems*, presentation at Workshop on Theory and Realisation of Practical Quantum Key Distribution 2007, Institute for Quantum Computing, University of Waterloo, Canada, available at http://www.iqc.ca/quantumworld/presentation_media/tropical_QKD/Lo.ppt.
31. P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård, and E. Polzik (2001), *Experimental quantum key distribution with proven security against realistic attacks*, *J. Modern Optics*, vol. 48, pp. 1921–1942.
32. M. J. LaGasse (2005), *Secure use of a single single-photon detector in a QKD system*, United States patent application 20050190922.
33. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy (2006), *Trojan-horse attacks on quantum-key-distribution systems*, *Phys. Rev. A*, vol. 73, p. 022320.

34. L. Lydersen and J. Skaar (2008), *Security of quantum key distribution with bit and basis dependent detector flaws*, {e-print}arXiv:0807.0767[quant-ph].
35. R. Gelles and T. Mor (2007), *Quantum-space attacks*, {e-print}arXiv:0711.3019[quant-ph].
36. K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim (2005), *General paradigm for distilling classical key from quantum states*, {e-print}arXiv:quant-ph/0506189.
37. A. Acín, N. Gisin, and Ll. Masanes (2006), *From Bell's theorem to secure quantum key distribution*, Phys. Rev. Lett., vol. 97, p. 120405.
38. V. Scarani, N. Gisin, N. Brunner, Ll. Masanes, S. Pino, and A. Acín (2006), *Secrecy extraction from no-signaling correlations*, Phys. Rev. A, vol. 74, p. 042339.
39. W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons (1998), *Free-space quantum-key distribution*, Phys. Rev. A, vol. 57, pp. 2379–2382.
40. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons (1998), *Practical free-space quantum key distribution over 1 km*, Phys. Rev. Lett., vol. 81, pp. 3283–3286.
41. W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson (2000), *Daylight quantum key distribution over 1.6 km*, Phys. Rev. Lett., vol. 84, pp. 5652–5655.
42. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson (2002), *Practical free-space quantum key distribution over 10 km in daylight and at night*, New J. Phys., vol. 4, p. 43.
43. C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan (2005), *Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication*, Phys. Rev. Lett., vol. 94, p. 150501.
44. I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer (2006), *Free-space quantum key distribution with entangled photons*, Appl. Phys. Lett., vol. 89, p. 101122.
45. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger (2007), *Entanglement-based quantum communication over 144 km*, Nature Physics, vol. 3, pp. 481–486.
46. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter (2007), *Experimental demonstration of free-space decoy-state quantum key distribution over 144 km*, Phys. Rev. Lett., vol. 98, p. 010504.
47. M. A. Albota and F. N. C. Wong (2004), *Efficient single-photon counting at 1.55 μ m by means of frequency upconversion*, Opt. Lett., vol. 29, pp. 1449–1451.
48. A. V. Oppenheim, A. S. Willsky, and S. H. Nawab, *Signals and Systems*, 2nd ed. Prentice Hall, 1996.
49. C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher (1996), *Concentrating partial entanglement by local operations*, Phys. Rev. A, vol. 53, pp. 2046–2052.
50. M. Curty, M. Lewenstein, and N. Lütkenhaus (2004), *Entanglement as a precondition for secure quantum key distribution*, Phys. Rev. Lett., vol. 92, p. 217903.
51. J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes (2005), *Unconditional security of three state quantum key distribution protocols*, Phys. Rev. Lett., vol. 94, p. 040503.
52. K. Tamaki and H.-K. Lo (2006), *Unconditionally secure key distillation from multiphotons*, Phys. Rev. A, vol. 73, p. 010302(R).
53. C.-H. F. Fung, K. Tamaki, and H.-K. Lo (2006), *Performance of two quantum-key-distribution protocols*, Phys. Rev. A, vol. 73, p. 012337.
54. K. Azuma (1967), *Weighted sums of certain dependent random variables*, Tôhoku Math. J., vol. 19, pp. 357–367.
55. C.-H. F. Fung and H.-K. Lo (2006), *Security proof of a three-state quantum key distribution protocol without rotational symmetry*, Phys. Rev. A, vol. 74, p. 042342.
56. K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe (2006), *Unconditional se-*

- curity of the Bennett 1992 quantum key-distribution scheme with strong reference pulse, {e-print}arXiv:quant-ph/0607082.
57. J. B. Lasserre (2001), *Global optimization with polynomials and the problem of moments*, SIAM J. Optimization, vol. 11, pp. 796–817.
 58. L. Vandenberghe and S. Boyd (1996), *Semidefinite programming*, SIAM Review, vol. 38, pp. 49–95.
 59. T. Tsurumaru and K. Tamaki (2008), *Security proof for quantum-key-distribution systems with threshold detectors*, Phys. Rev. A, vol. 78, p. 032302.
 60. N. J. Beaudry, T. Moroder, and N. Lütkenhaus (2008), *Squashing models for optical measurements in quantum communication*, Phys. Rev. Lett., vol. 101, p. 093601.
 61. H.-K. Lo, H. F. Chau, and M. Ardehali (2005), *Efficient quantum key distribution scheme and a proof of its unconditional security*, J. of Cryptology, vol. 18, pp. 133–165.
 62. T. Moroder, M. Curty, and N. Lütkenhaus (2008), *Detector decoy quantum key distribution*, presentation at Information Security in a Quantum World, Institute for Quantum Computing, University of Waterloo, Canada.
 63. W.-Y. Hwang (2003), *Quantum key distribution with high loss: Toward global secure communication*, Phys. Rev. Lett., vol. 91, p. 057901.
 64. H.-K. Lo, X. Ma, and K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett., vol. 94, p. 230504.
 65. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo (2005), *Practical decoy state for quantum key distribution*, Phys. Rev. A, vol. 72, p. 012326.
 66. X.-B. Wang (2005), *Beating the photon-number-splitting attack in practical quantum cryptography*, Phys. Rev. Lett., vol. 94, p. 230503.
 67. X.-B. Wang (2005), *Decoy-state protocol for quantum cryptography with four different intensities of coherent light*, Phys. Rev. A, vol. 72, p. 012322.
 68. J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt (2005), *Enhancing practical security of quantum key distribution with a few decoy states*, {e-print}arXiv:quant-ph/0503002.
 69. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian (2006), *Experimental quantum key distribution with decoy states*, Phys. Rev. Lett., vol. 96, p. 070502.
 70. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber*, in *Proc. of IEEE Int'l Symp. Information Theory (ISIT) 2006*. IEEE Press, New York, July 2006, pp. 2094–2098.

Appendix A: Analysis of time-dependent efficiency

Here, we justify that the efficiency response of a detector can be characterized with a finite number of samples when a narrow-band filter is placed before the detector.

Before we begin, we remark that we will work on the baseband signals, even though the signals are modulated to a higher carrier frequency before detection. This is valid because practical detectors are not fast enough to respond to the optical frequency of the input signal. So only the envelope of the signal, which is equivalent to the baseband of the signal, will be detected. Thus, with this built-in demodulation function in the detectors, we can work on the baseband signals.

Suppose that the input (quantum) signal at the detector location is $E(t)$, and the Gaussian-shaped frequency filter is $g(f)$ and has an effective bandwidth of B . Since the filter has a fixed bandwidth, we can assume without loss of generality that the input signal also has a fixed bandwidth B . Then the input signal in the frequency domain can be expressed as

$$E(f) = [E(f) * \sum_{k=-\infty}^{\infty} \delta(f - 2Bk)]h(f) \quad (\text{A.1})$$

where $h(f)$ is the perfect rectangular filter with bandwidth B , and the asterisk denotes convolution. Here, we are essentially repeating $E(f)$ indefinitely with a separation of $2B$ and then chopping the spectrum with the low-pass filter $h(f)$. This can be seen by noting that $E(f) * \delta(f - 2B) = E(f - 2B)$. This step may look superfluous, but the reason for this will be clear when we look at the time domain. The output of the filter is, in the frequency domain,

$$E'(f) = E(f)g(f) \quad (\text{A.2})$$

$$= [E(f) * \sum_{k=-\infty}^{\infty} \delta(f - 2Bk)]g(f) \quad (\text{A.3})$$

where we have used the fact that $g(f) = g(f)h(f)$. In the time domain, the output is obtained through the Fourier transform:

$$E'(t) = (2B)^{-1} [E(t) \sum_{k=-\infty}^{\infty} \delta(t - k/(2B))] * g(t). \quad (\text{A.4})$$

Here, we have used the convolution property of the Fourier transform which says that convolution in the time domain becomes multiplication in the frequency domain and vice versa. Also, we used the fact that the Fourier transform of an impulse train is also an impulse train, i.e.,

$$\sum_{k=-\infty}^{\infty} \delta(f - 2Bk) \leftrightarrow (2B)^{-1} \sum_{k=-\infty}^{\infty} \delta(t - k/(2B)) \quad (\text{A.5})$$

are a Fourier transform pair. Finally, we expand the convolution in Eq. (A.4) to get

$$E'(t) = (2B)^{-1} \sum_{k=-\infty}^{\infty} E(k/(2B))g(t - k/(2B)). \quad (\text{A.6})$$

This last equation illustrates the key point, which is that given any input signal $E(t)$, the output of the filter can always be represented by a train of Gaussian pulses (possibly with different amplitudes) spaced at $1/(2B)$ time intervals. Thus, the detector always receives a train of Gaussian pulses located at fixed time instants and if the fixed length of the gating window is taken into account, one can characterize the detector with a finite number of pulses sent within the gating window. Therefore, the detection efficiency response $F_i^\dagger F_i$ effectively becomes finite dimensional. This proves that with an addition of a frequency filter, the characterization of the time-dependent efficiency of the detectors becomes discrete and finite-dimensional, and thus is readily applicable to our security proof. Note that although our analysis does not explicitly involve quantum mechanics, the analysis is still applicable to quantum states since the Fourier transform is an unitary transformation (also linear) that changes between the time basis and the frequency basis, and the quantities $E(f)$ and $E(t)$ can be regarded as the amplitudes of a quantum state in the respective basis.

Appendix B: Determination of Bob's virtual filter for the noiseless case

We determine Bob's virtual filter G_{BT} in Eq. (9) by finding the matrix $C \in \mathbb{C}^{d \times d}$. Since a valid filter G_{BT} must satisfy $G_{BT}^\dagger G_{BT} \leq I$, we find C such that this is satisfied while

maximizing the key generation rate in Eq. (13). This problem can be expressed as

$$\max_C \min_{|\gamma\rangle} \frac{2 \langle \gamma | (C^\dagger C)_T \otimes I_E | \gamma \rangle_{TE}}{\langle \gamma | (F_0^\dagger F_0 + F_1^\dagger F_1)_T \otimes I_E | \gamma \rangle_{TE}} \quad (\text{B.1})$$

$$s.t. \quad G_{BT}^\dagger G_{BT} \leq I. \quad (\text{B.2})$$

Note that since we are interested in the worst-case key generation rate, we form a max-min problem as opposed to a min-max problem, in light of the max-min inequality: $\max_a \min_b f(a, b) \leq \min_b \max_a f(a, b)$.

To solve this optimization problem, first note that the condition $G_{BT}^\dagger G_{BT} \leq I$ is the same as the condition $G_{BT} G_{BT}^\dagger \leq I$, which can be expanded (by using Eq. (9)) as

$$|0_z\rangle_B \langle 0_z| \otimes C(F_0^\dagger F_0)^{-1} C^\dagger + |1_z\rangle_B \langle 1_z| \otimes C(F_1^\dagger F_1)^{-1} C^\dagger \leq I. \quad (\text{B.3})$$

Letting $C = C_1 U^\dagger F_0$ where $C_1 \in \mathbb{C}^{d \times d}$ will be determined next, $U \in \mathbb{C}^{d \times d}$ is the unitary matrix of the Hermitian decomposition of $F_0(F_1^\dagger F_1)^{-1} F_0^\dagger = U D U^\dagger$, and $D = \text{diag}(D_1, \dots, D_d)$ is a diagonal matrix with positive real elements, Eq. (B.3) can be expressed as

$$|0_z\rangle_B \langle 0_z| \otimes C_1 C_1^\dagger + |1_z\rangle_B \langle 1_z| \otimes C_1 D C_1^\dagger \leq I. \quad (\text{B.4})$$

This allows us to redefine the constraints of the problem.

Next, we consider the objective function in Eq. (B.1), which can be simplified as

$$\frac{2 \langle \gamma | (C^\dagger C)_T | \gamma \rangle}{\langle \gamma | (F_0^\dagger F_0 + F_1^\dagger F_1)_T | \gamma \rangle} \quad (\text{B.5})$$

$$= \frac{2 \langle \gamma' | (F_0^{\dagger^{-1}} C^\dagger C F_0^{-1})_T | \gamma' \rangle}{\langle \gamma' | (I + F_0^{\dagger^{-1}} F_1^\dagger F_1 F_0^{-1})_T | \gamma' \rangle} \quad (\text{B.6})$$

$$= \frac{2 \langle \gamma'' | (C_1^\dagger C_1)_T | \gamma'' \rangle}{\langle \gamma'' | (I + D^{-1})_T | \gamma'' \rangle} \quad (\text{B.7})$$

$$= \frac{2 \langle \gamma''' | ((I + D^{-1})^{-1/2} C_1^\dagger C_1 (I + D^{-1})^{-1/2})_T | \gamma''' \rangle}{\langle \gamma''' | \gamma''' \rangle}. \quad (\text{B.8})$$

Now, the problem can be re-written as

$$R_{\text{noiseless}} = \max_{C_2} \min_{|\gamma\rangle} \frac{2 \langle \gamma | (C_2^\dagger C_2)_T \otimes I_E | \gamma \rangle_{TE}}{\langle \gamma | \gamma \rangle} \quad (\text{B.9})$$

$$s.t. \quad C_2(I + D^{-1})C_2^\dagger \leq I \quad (\text{B.10})$$

$$C_2(I + D)C_2^\dagger \leq I \quad (\text{B.11})$$

where $C_2 = C_1(I + D^{-1})^{-1/2}$. We further simplify the problem as

$$R_{\text{noiseless}} = 2 \max_{C_2} [\text{minimum eigenvalue of } C_2^\dagger C_2] \quad (\text{B.12})$$

$$s.t. \quad C_2 \begin{bmatrix} 1 + \frac{1}{D_1} & & \\ & \ddots & \\ & & 1 + \frac{1}{D_d} \end{bmatrix} C_2^\dagger \leq I \quad (\text{B.13})$$

$$C_2 \begin{bmatrix} 1 + D_1 & & \\ & \ddots & \\ & & 1 + D_d \end{bmatrix} C_2^\dagger \leq I. \quad (\text{B.14})$$

The solution is

$$C_2 = \begin{bmatrix} \sqrt{\min\left(\frac{1}{1+D_1}, \frac{D_1}{1+D_1}\right)} & & \\ & \ddots & \\ & & \sqrt{\min\left(\frac{1}{1+D_d}, \frac{D_d}{1+D_d}\right)} \end{bmatrix} \quad (\text{B.15})$$

$$C = \begin{bmatrix} \sqrt{\min\left(\frac{1}{D_1}, 1\right)} & & \\ & \ddots & \\ & & \sqrt{\min\left(\frac{1}{D_d}, 1\right)} \end{bmatrix} U^\dagger F_0, \quad (\text{B.16})$$

and the final key generation rate can be obtained by substituting Eq. (B.15) into Eq. (B.12):

$$\begin{aligned} R_{\text{noiseless}} &= 2 \min \left(\frac{1}{1+D_1}, \frac{1}{1+1/D_1}, \frac{1}{1+D_2}, \dots \right) \\ &= \frac{2}{1 + \max \left(D_1, \frac{1}{D_1}, \dots, D_d, \frac{1}{D_d} \right)}. \end{aligned}$$

Appendix C: Simplification of Eqs. (19)-(22)

Here, we show how to simplify e_b in Eq. (19). The other quantities in Eqs. (20)-(22) can be similarly simplified.

Let's re-write Eq. (16) by separating the operations for systems B and T by expressing $E_{BT}^{(l,i)} = \sum_j E_B^{(l,i,j)} \otimes E_T^{(l,i,j)}$:

$$|\Psi_2^{(l)}\rangle = \sum_{i,j} E_B^{(l,i,j)} (|00\rangle + |11\rangle)_{AB} \otimes |\gamma^{(l,i,j)}\rangle_T \otimes |i\rangle_E \quad (\text{C.1})$$

where $|\gamma^{(l,i,j)}\rangle = E_T^{(l,i,j)} |0\rangle$. Consider Eq. (17) which is expanded as

$$\begin{aligned} F_z |\Psi_2^{(l)}\rangle &= \sum_{i,j} \left\{ \left[a_{00}^{(l,i,j)} |00\rangle_{AB} + a_{10}^{(l,i,j)} |10\rangle_{AB} \right] \otimes F_0 |\gamma^{(l,i,j)}\rangle_T + \right. \\ &\quad \left. \left[a_{01}^{(l,i,j)} |01\rangle_{AB} + a_{11}^{(l,i,j)} |11\rangle_{AB} \right] \otimes F_1 |\gamma^{(l,i,j)}\rangle_T \right\} \otimes |i\rangle_E \end{aligned} \quad (\text{C.2})$$

where

$$a_{00}^{(l,i,j)} = \frac{a_I^{(l,i,j)} + a_Z^{(l,i,j)}}{\sqrt{2}} \quad a_{01}^{(l,i,j)} = \frac{a_X^{(l,i,j)} - a_Y^{(l,i,j)}}{\sqrt{2}} \quad (\text{C.3})$$

$$a_{10}^{(l,i,j)} = \frac{a_X^{(l,i,j)} + a_Y^{(l,i,j)}}{\sqrt{2}} \quad a_{11}^{(l,i,j)} = \frac{a_I^{(l,i,j)} - a_Z^{(l,i,j)}}{\sqrt{2}} \quad (\text{C.4})$$

and Eve's operation is expressed in terms of the Pauli matrices as $E_B^{(l,i,j)} = a_I^{(l,i,j)} I + a_X^{(l,i,j)} X + a_Y^{(l,i,j)} iY + a_Z^{(l,i,j)} Z$. Using this notation in Eq. (19), we have

$$e_b = \frac{\sum_{l,i,j,j'} a_{10}^{J'\dagger} a_{10}^J \langle \gamma^{J'} | F_0^\dagger F_0 | \gamma^J \rangle + a_{01}^{J'\dagger} a_{01}^J \langle \gamma^{J'} | F_1^\dagger F_1 | \gamma^J \rangle}{\sum_{l,i,j,j'} (a_{10}^{J'\dagger} a_{10}^J + a_{00}^{J'\dagger} a_{00}^J) \langle \gamma^{J'} | F_0^\dagger F_0 | \gamma^J \rangle + (a_{01}^{J'\dagger} a_{01}^J + a_{11}^{J'\dagger} a_{11}^J) \langle \gamma^{J'} | F_1^\dagger F_1 | \gamma^J \rangle} \quad (\text{C.5})$$

where, for simplicity, J' means (l, i, j') and J means (l, i, j) . Focusing on the first term in the numerator with fixed l and i , it is equal to

$$\begin{aligned} & \sum_{j,j'} a_{10}^{J'\dagger} a_{10}^J \langle \gamma^{J'} | F_0^\dagger F_0 | \gamma^J \rangle \\ &= \left(\langle \gamma^{(l,i,0)} | \quad \langle \gamma^{(l,i,1)} | \quad \dots \right) \left[\begin{pmatrix} a_{10}^{(l,i,0)\dagger} a_{10}^{(l,i,0)} & a_{10}^{(l,i,0)\dagger} a_{10}^{(l,i,1)} & \dots \\ a_{10}^{(l,i,1)\dagger} a_{10}^{(l,i,0)} & \ddots & \\ \vdots & & \end{pmatrix} \otimes F_0^\dagger F_0 \right] \begin{pmatrix} |\gamma^{(l,i,0)}\rangle \\ |\gamma^{(l,i,1)}\rangle \\ \vdots \end{pmatrix}. \end{aligned} \quad (\text{C.6})$$

The second matrix can immediately be recognized as $A^{(l,i)\dagger} \tilde{Z}_{10} A^{(l,i)}$ where \tilde{Z}_{10} is from Eq. (C.11) below and

$$A^{(l,i)} = \begin{pmatrix} a_I^{(l,i,0)} & a_I^{(l,i,1)} & \dots \\ a_X^{(l,i,0)} & a_X^{(l,i,1)} & \dots \\ a_Y^{(l,i,0)} & a_Y^{(l,i,1)} & \dots \\ a_Z^{(l,i,0)} & a_Z^{(l,i,1)} & \dots \end{pmatrix}. \quad (\text{C.8})$$

By letting

$$|\phi(l, i)\rangle = (A^{(l,i)} \otimes I) \begin{pmatrix} |\gamma^{(l,i,0)}\rangle \\ |\gamma^{(l,i,1)}\rangle \\ \vdots \end{pmatrix} \quad (\text{C.9})$$

where the identity matrix has dimensions $d \times d$ and applying similar arguments to other terms, we have

$$e_b = \frac{\sum_{l,i} \langle \phi(l, i) | [\tilde{Z}_{10} \otimes F_0^\dagger F_0 + \tilde{Z}_{01} \otimes F_1^\dagger F_1] | \phi(l, i) \rangle}{\sum_{l,i} \langle \phi(l, i) | [(\tilde{Z}_{00} + \tilde{Z}_{10}) \otimes F_0^\dagger F_0 + (\tilde{Z}_{11} + \tilde{Z}_{01}) \otimes F_1^\dagger F_1] | \phi(l, i) \rangle} \quad (\text{C.10})$$

where $\tilde{Z}_{i,j}$ are constant matrices shown below in Eq. (C.11). Finally, by letting $\rho_E = \sum_{l,i} |\phi(l, i)\rangle \langle \phi(l, i)|$, Eq. (C.10) becomes Eq. (23). Similarly, Eqs. (20)-(22) can be simplified

where $\tilde{Z}_{i,j}$ and $\tilde{X}_{i,j}$ are

$$\begin{aligned}\tilde{Z}_{00} &= P([1, 0, 0, 1]^\dagger)/2 & \tilde{X}_{++} &= P([1, 1, 0, 0]^\dagger)/2 \\ \tilde{Z}_{10} &= P([0, 1, 1, 0]^\dagger)/2 & \tilde{X}_{-+} &= P([0, 0, -1, 1]^\dagger)/2 \\ \tilde{Z}_{01} &= P([0, 1, -1, 0]^\dagger)/2 & \tilde{X}_{+-} &= P([0, 0, 1, 1]^\dagger)/2 \\ \tilde{Z}_{11} &= P([1, 0, 0, -1]^\dagger)/2 & \tilde{X}_{--} &= P([1, -1, 0, 0]^\dagger)/2.\end{aligned}\tag{C.11}$$

Here, $P(|\cdot\rangle) = |\cdot\rangle\langle\cdot|$ is the projection operator.

Appendix D: Solving for the suboptimal bounds

Here, we prove Eqs. (27) and (28). First, we consider solving

$$p_{\text{succ, noisy}} \geq \min_{|\phi\rangle} \frac{\langle\phi| I \otimes C^\dagger C |\phi\rangle}{\langle\phi| [(\tilde{Z}_{00} + \tilde{Z}_{10}) \otimes F_0^\dagger F_0 + (\tilde{Z}_{11} + \tilde{Z}_{01}) \otimes F_1^\dagger F_1] |\phi\rangle}\tag{D.1}$$

where the right hand side comes from Eq. (26) and $\tilde{Z}_{00} + \tilde{Z}_{10} + \tilde{Z}_{11} + \tilde{Z}_{01} = I$. Here, we only need to focus on rank-one $\rho_E = |\phi\rangle\langle\phi|$ because of the following claim.

Claim 1 Given two ratios, $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$, where $a_1, a_2, b_1, b_2 \in \mathbb{R}_+$, if $\frac{a_1}{a_2} \geq \frac{b_1}{b_2}$, then $\frac{a_1}{a_2} \geq \frac{a_1+b_1}{a_2+b_2}$. Similarly, if $\frac{a_1}{a_2} \leq \frac{b_1}{b_2}$, then $\frac{a_1}{a_2} \leq \frac{a_1+b_1}{a_2+b_2}$.

This claim basically means that we only need to focus on the smallest or the largest ratio when there are more than one ratio to optimize over. By substituting $|\phi'\rangle = [(\tilde{Z}_{00} + \tilde{Z}_{10}) \otimes F_0 + (\tilde{Z}_{11} + \tilde{Z}_{01}) \otimes F_1] |\phi\rangle$ into the right hand side of Eq. (D.1), we get

$$p_{\text{succ, noisy}} \geq \min_{|\phi\rangle} \frac{\langle\phi'| [(\tilde{Z}_{00} + \tilde{Z}_{10}) \otimes F_0^{-\dagger} C^\dagger C F_0^{-1} + (\tilde{Z}_{11} + \tilde{Z}_{01}) \otimes F_1^{-\dagger} C^\dagger C F_1^{-1}] |\phi'\rangle}{\langle\phi'| \phi'\rangle}.\tag{D.2}$$

By noting that $\tilde{Z}_{00} + \tilde{Z}_{10}$ and $\tilde{Z}_{11} + \tilde{Z}_{01}$ are orthogonal, the minimum eigenvalue of Eq. (D.2) is the minimum of the eigenvalues of $F_i^{-\dagger} C^\dagger C F_i^{-1}$ where $i = 0, 1$. By using Eq. (B.16), one can immediately see that the eigenvalues of $F_0^{-\dagger} C^\dagger C F_0^{-1}$ are

$$\min\left(\frac{1}{D_i}, 1\right) \quad i = 1, \dots, d\tag{D.3}$$

and that of $F_1^{-\dagger} C^\dagger C F_1^{-1}$ are

$$\min(D_i, 1) \quad i = 1, \dots, d.\tag{D.4}$$

Taking the minimum of these two sets of eigenvalues gives Eq. (27).

Next, we consider the maximization of e_p/e'_p in Eq. (28). Using Eqs. (24) and (25) (and Claim 1), we have

$$\begin{aligned}\frac{e_p}{e'_p} &= \frac{\langle\phi| \tilde{X}_{-+} \otimes C^\dagger C |\phi\rangle + \langle\phi| \tilde{X}_{+-} \otimes C^\dagger C |\phi\rangle}{\langle\phi| \tilde{X}_{-+} \otimes F_0^\dagger F_0 |\phi\rangle + \langle\phi| \tilde{X}_{+-} \otimes F_1^\dagger F_1 |\phi\rangle} \times \\ &\quad \frac{\langle\phi| (\tilde{X}_{++} + \tilde{X}_{-+}) \otimes F_0^\dagger F_0 |\phi\rangle + \langle\phi| (\tilde{X}_{--} + \tilde{X}_{+-}) \otimes F_1^\dagger F_1 |\phi\rangle}{\langle\phi| (\tilde{X}_{++} + \tilde{X}_{-+}) \otimes C^\dagger C |\phi\rangle + \langle\phi| (\tilde{X}_{--} + \tilde{X}_{+-}) \otimes C^\dagger C |\phi\rangle}.\end{aligned}\tag{D.5}$$

According to Claim 1, the first ratio in Eq. (D.5) is upper bounded by the maximum of the eigenvalues of $F_i^{-\dagger} C^\dagger C F_i^{-1}$ where $i = 0, 1$; while the second ratio is upper bounded by inverse of the minimum of the same set of eigenvalues. Therefore, using Eqs. (D.3)-(D.4),

$$\frac{e_p}{e'_p} \leq \frac{1}{\min \left(D_1, \frac{1}{D_1}, \dots, D_d, \frac{1}{D_d}, 1 \right)} \quad (\text{D.6})$$

where the numerator ($= 1$) corresponds to the upper bound on the first ratio. This proves Eq. (28).